Спільна програма Європейського Союзу та Ради Європи
«Зміцнення інформаційного суспільства в Україні»

Фінансується
Європейським Союзом
та Радою Європи

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Впроваджується
Радою Європи

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА ПРАКТИЧНІ АСПЕКТИ

Науково-практичний посібник

Це видання опубліковано в рамках спільної програми Ради Європи та Європейського Союзу «Зміцнення інформаційного суспільства в Україні». Погляди, виражені в даній публікації, відображають позицію авторів та не обов'язково відображають офіційну позицію Ради Європи та Європейського Союзу.

Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М.
Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.

ISBN 978-617-684-129-6

Посібник складено за програмою навчального курсу «Захист персональних даних: правове регулювання та практичні аспекти», що спрямований на підвищення рівня обізнаності щодо регулювання захисту персональних даних та процесу їх обробки в Україні. У посібнику викладені основні юридичні інструменти регулювання захисту персональних даних та порядок і процедури їх застосування.

Видано Радою Європи.
F-67075 Strasbourg Cedex
www.coe.int

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

Рада Європи – це міжурядова організація, до якої входить 47 держав-членів, завданням якої є захищати права людини, плюралістичну демократію та верховенство права; сприяти усвідомленню та оцінці європейської культурної самобутності та розмаїття європейських культур; знаходити вирішення проблем, що існують у суспільстві (ксенофобія, нетерпимість, захист навколишнього середовища, клонування, СНІД, наркотики, організована злочинність і т. ін.); допомагати стверджувати стабільність демократії у Європі через підтримку політичних, законотворчих та конституційних реформ. Більше інформації про Офіс Ради Європи в Україні: http://www.coe.int/en/web/kyiv.

Спільна програма Європейського Союзу та Ради Європи «Зміцнення інформаційного суспільства в Україні» має на меті покращити свободу, різноманітність і плюралізм медіа, а також сприяти ефективності системи захисту персональних даних. Також програма спрямована на відкритий, всебічний і сталий підхід до управління Інтернетом, що ґрунтується на правах людини і ставить людину в центр уваги. Крім того, програма сприятиме виконанню обов'язків і зобов'язань України перед Радою Європи, реалізації Угоди про асоціацію з ЄС і Плану дій з лібералізації ЄС візового режиму для України. Більше інформації про програму: http://www.coe.int/en/web/kyiv/41.

ISBN 978-617-684-129-6

ЗМІСТ

ПЕРЕДМОВА

Шановні читачі!

Початок XXI століття ознаменувався новим витком розвитку інформаційних технологій, які стають невід'ємною частиною нашого з Вами повсякденного життя. Технологічний прогрес створює все ширше коло потреб та можливостей для збору та обробки персональних даних, а самі персональні дані знаходять все ширше використання в найрізноманітніших сферах від бізнесу до політики. Їх використання стає багатоаспектнішим і, окрім допомоги в роботі та побуті, вони можуть слугувати для декого інструментом порушення прав та свобод людини, зокрема права на приватність.

У зв'язку з цим, розвиток системи захисту персональних даних є одним із найбільш актуальних завдань, які стоять перед українським суспільством на сучасному етапі. Захист персональних даних та його вдосконалення є не просто обов'язком держави і предметом державно-правового регулювання, але повинні нерозривно розглядатися в поєднанні зі захистом прав та свобод людини, в тому числі захистом права на повагу до приватного життя. Крім того, створення дієвої системи захисту персональних даних належить до міжнародних зобов'язань України, в тому числі пов'язаних із європейською інтеграцією нашої держави. Зокрема, саме від виконання цього зобов'язання значною мірою залежать євроінтеграційні прагнення української держави.

Ефективність такої системи захисту персональних даних, окрім правових інструментів, які її регулюють, сьогодні забезпечується високопрофесійною діяльністю уповноважених органів у цій сфері, які вже досягли вагомих успіхів у справі імплементації міжнародних та європейських стандартів захисту персональних даних. Однак, важливим фактором також є рівень обізнаності громадян та суспільних акторів щодо шляхів та можливостей застосування цих

інструментів. Як свідчить українська дійсність, громадяни часто ігнорують проблеми пов'язані зі захистом власних персональних даних, у тому числі через неповне розуміння законодавчих стандартів та вимог у цій сфері.

Саме підвищення рівня обізнаності громадськості щодо правових засад захисту персональних даних в Україні є одним із пріоритетних напрямків подальшого розвитку цієї системи. Окрім поширення знань та відомостей про персональні дані широкому загалу, передбачається підготовка кола фахівців, які володітимуть професійними знаннями та вміннями у цій сфері.

Така підготовка експертів має відбуватися системно на основі уніфікованих підходів до вивчення та розуміння захисту персональних даних не просто як до системи правових норм, а й як до системи інструментів, які регулярно повинні застосуватися у ході суспільних відносин.

Впевнена, що саме їхні активна позиція та професійні навички стануть тим ключем до змін, яких так потребує Україна в цій сфері.

Валерія Лутковська,
Уповноважений Верховної Ради з прав людини

КОРОТКИЙ ВИКЛАД ОСНОВНИХ РОЗДІЛІВ ПОСІБНИКА

ТЕМА 1. ПОНЯТТЯ «ПЕРСОНАЛЬНІ ДАНІ» ТА ДЖЕРЕЛА ЇХ ПРАВОВОГО РЕГУЛЮВАННЯ.

Джерела правового регулювання відносин зі захисту персональних даних. Регулювання захисту персональних даних у міжнародно-правових нормах щодо права на приватність. Захист персональних даних у правових актах Ради Європи та Європейського Союзу. Національне законодавство України зі захисту персональних даних. Закон України «Про захист персональних даних». Нормативно-правові акти Уповноваженого Верховної Ради з прав людини щодо захисту персональних даних.

Визначення поняття «персональні дані» в законодавстві України. Поняття «ідентифікована особа» як ключове для розуміння поняття «персональні дані». Класифікація видів персональних даних. Чутливі (спеціальні) категорії персональних даних.

Поняття обробки персональних даних. Співвідношення понять «обробка», «захист» та «використання» персональних даних. Проблеми визначення та співвідношення понять «обробка», «захист» та «використання» персональних даних у Законі України «Про захист персональних даних». Обробка персональних даних у приватних, журналістських та творчих цілях. Поняття знеособлення персональних даних.

Поняття володільця персональних даних. Поняття розпорядника персональних даних. Співвідношення понять «володілець» та «розпорядник» персональних даних. Поняття «третя особа» у відносинах із приводу захисту персональних даних. Поняття «одержувач персональних даних». Уповноважений Верховної Ради з прав людини у відносинах щодо захисту персональних даних.

ТЕМА 2. ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ.

Поняття та види принципів обробки персональних даних. Закріплення принципів обробки персональних даних у Законі України «Про захист персональних даних». Принципи захисту персональних даних у практиці Європейського Суду з прав людини.

Принцип законності обробки персональних даних. Мета та підстави обробки персональних даних відповідно до принципу законності. Застосування принципу законності в рішенні ЄСПЛ у справі «Ротару проти Румунії».

Принцип визначеності мети обробки персональних даних. Критерії визначення мети обробки персональних даних. Застосування принципу законності в рішенні ЄСПЛ у справі «М.К. проти Румунії». Зміна визначеної мети обробки персональних даних. Обробка персональних даних з науковою, статистичною та/чи історичною метою і гарантії, що даються при такій обробці.

Принцип адекватності, відповідності та ненадмірності. Значення принципу адекватності, відповідності та ненадмірності в процесі обробки персональних даних. Принцип адекватності, відповідності та ненадмірності в рішенні ЄСПЛ у справі «Гардель проти Франції». Застереження щодо застосування принципу адекватності, відповідності та ненадмірності на підставі згоди особи.

Принципи достовірності та точності. Принцип чесності обробки персональних даних.

ТЕМА 3. ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ.

Загальна характеристика підстав обробки персональних даних. Види підстав обробки персональних даних: згода суб'єкта і на підставі закону. Диференціація понять «обробка на підставі закону» та «законність (легітимність) обробки».

Статус персональних даних. Співвідношення понять «персональні дані» та «конфіденційна інформація». Конфіденційна інформація та законодавче регулювання її статусу. Підстави обробки конфіденційної інформації про особу.

Згода суб'єкта персональних даних як підстава для їх обробки. Ознаки «згоди суб'єкти» як підстави для обробки персональних даних. Укладення та виконання правочину як підстава для обробки персональних даних. Закон як підстава для обробки персональних

даних. Практика ЄСПЛ щодо застосування закону як підстави обробки персональних даних у рішеннях у справах «Зайченко проти України» та «П.Г. проти Об'єднаного Королівства».

Обробка персональних даних у цілях захисту життєво важливих інтересів суб'єкта персональних даних. Обробка персональних даних у цілях необхідності виконання обов'язку володільця персональних даних, який передбачений законом. Обробка персональних даних у цілях необхідності 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.

Підстави обробки чутливих категорій персональних даних та їх види. Особливості правового регулювання обробки персональних даних у медичних цілях. Практика ЄСПЛ щодо обробки персональних даних у медичних цілях у рішеннях у справах «Л.Х. проти Латвії», «Авілкіна та інші проти Росії», «Л. проти Фінляндії», «З. проти Фінляндії».

ТЕМА 4. ПРАВА СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ ТА ШЛЯХИ ЇХ РЕАЛІЗАЦІЇ (ДОСТУП ДО ІНФОРМАЦІЇ ПРО СЕБЕ; ДОСТУП ДО ІНФОРМАЦІЇ ПРО ТРЕТІХ ОСІБ; ПРАВО НА ЗМІНУ, МОДИФІКАЦІЮ, ВИДАЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ; ПРАВО ЗНАТИ ПРО ПОРЯДОК ОБРОБКИ, АДЕКВАТНИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ).

Зобов'язання володільця персональних даних згідно із законом. Зобов'язання володільця персональних даних щодо інформування суб'єкта персональних даних про їх обробку. Права суб'єкта персональних даних у випадку подання запиту до володільця. Зобов'язання володільця щодо збереження інформації про передачу персональних даних суб'єкта. Право суб'єкта персональних даних пред'являти вимоги щодо зміни або знищення своїх персональних даних. Інші права суб'єкта персональних даних відповідно до Закону України «Про захист персональних даних».

ТЕМА 5. ОБМЕЖЕННЯ ДІЇ ПРАВ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ.

Випадки обмеження дії прав суб'єктів персональних даних. Обмеження дії прав суб'єктів персональних даних відповідно до положень Конвенції №108 Ради Європи про автоматизовану обробку персональних даних. Обмеження дії прав суб'єкта персональних даних відповідно до Закону України «Про захист персональних даних. Критерії, які пред'являються до обмежень дії прав суб'єкта персональних даних. Державна таємниця як підстава обмеження дії прав суб'єкта персональних даних.

ТЕМА 6. ПОРЯДОК ОРГАНІЗАЦІЇ ВОЛОДІЛЬЦЕМ ПРОЦЕСУ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

Поняття захисту персональних даних. Зобов'язання володільця та його працівників зі захисту персональних даних. Обов'язкові засоби захисту персональних даних відповідно до законодавства України. Доступ працівників володільця до персональних даних та його отримання. Заходи зі захисту персональних даних у разі автоматизованої обробки персональних даних. Правила захисту персональних даних за умовчанням (англ. privacy by default).

Зобов'язання володільця перед суб'єктом персональних даних стосовно інформування про стан обробки персональних даних. Права суб'єкта персональних даних щодо отримання інформації про обробку своїх персональних даних.

Статус осіб та структурних підрозділів, відповідальних за захист персональних даних. Компетенція та повноваження таких осіб та структурних підрозділів. Види і порядок обробки та захисту персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних.

ТЕМА 7. ПОРЯДОК ПОВІДОМЛЕННЯ УПОВНОВАЖЕНОГО ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ, ЯКА СТАНОВИТЬ ОСОБЛИВИЙ РИЗИК ДЛЯ ПРАВ І СВОБОД СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ.

Поняття обробки персональних даних, що становить особливий ризик для прав і свобод суб'єктів. Зобов'язання володільця із пові-

домлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних. Порядок здійснення такого повідомлення відповідно до законодавства України. Винятки зі зобов'язання володільця із повідомлення Уповноваженого про здійснення ним будь-яких видів обробки персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних. Недоліки чинної процедури здійснення такого повідомлення.

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

Органи державної влади в Україні, які здійснюють контроль за додержанням законодавства в сфері захисту персональних даних. Повноваження Уповноваженого Верховної Ради з прав людини зі здійснення контролю за додержанням законодавства в сфері захисту персональних даних. Статус Представника Уповноваженого з питань захисту персональних даних та Департаменту з питань захисту персональних даних.

Повноваження Уповноваженого Верховної Ради з прав людини зі здійснення перевірок володільців персональних даних. Види таких перевірок та порядок їх проведення. Правові наслідки проведення перевірок.

Адміністративна відповідальність за порушення законодавства в сфері захисту персональних даних. Право на відшкодування збитків, заподіяних неналежною обробкою персональних даних.

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

Статус володільця персональних даних. Зобов'язання володільця з обробки персональних даних. Зобов'язання володільця з інформування про обробку персональних даних. Зобов'язання володільця та його працівників із вжиття заходів стосовно порядку захисту персональних даних. Розгляд володільцем звернень суб'єктів персональних даних щодо припинення обробки/зміни їх персональних даних. Регламентування володільцем порядку захисту персональних даних.

ТЕМА 10. ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ.

Посилення спроможності наглядового органу щодо захисту персональних даних у світовій мережі. Впровадження чіткого визначення того, як співвідносяться поняття «конфіденційна інформація» та «персональні дані». Необхідність приведення статей 7 та 11 Закону до положень Директиви та проекту Регламенту ЄС. Внесення змін до Закону в частині більш чіткого визначення згоди на обробку персональних даних. Внесення змін до законодавства в частині використання персональних даних. Пропозиції щодо змін у компетенції Уповноваженого у сфері захисту персональних даних. Реформа системи повідомлення. Перегляд випадків визначення структурного підрозділу або відповідальної особи, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці. Запровадження детальних положень щодо порядку реалізації прав суб'єктів персональних даних. Розмежування понять доступу та передачі/розкриття/поширення/оприлюднення. Узгодження Закону України «Про захист персональних даних» та Закону України «Про доступ до публічної інформації». Деталізація врегулювання відносин між володільцем та розпорядником.

ТЕМА 11. ТЕНДЕНЦІЇ РОЗВИТКУ СВІТОВОЇ ТА ЄВРОПЕЙСЬКОЇ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

Тенденції розвитку європейського права в сфері захисту персональних даних. Проект Регламенту ЄС щодо захисту персональних даних. Основні положення та новели проекту нового Регламенту ЄС про захист персональних даних. Перспективи гармонізації законодавства України в сфері захисту персональних даних із новим Регламентом ЄС.

ПОСІБНИК
ДО НАВЧАЛЬНОГО КУРСУ

ТЕМА 1. ПОНЯТТЯ «ПЕРСОНАЛЬНІ ДАНІ» ТА ДЖЕРЕЛА ЇХ ПРАВОВОГО РЕГУЛЮВАННЯ.

1.1. ДЖЕРЕЛА ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

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 «Керівні принципи зі 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 у сфері 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.

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». Саме цей документ і став джерелом тієї системи захисту персональних даних, якою вона є сьогодні. Так, заснований Конвенцією Європейський суд з прав людини у своєму рішенні у справі «Леандер проти Швеції» вперше зазначив, що зберігання державними органами інформації про особу є втручанням у її право на повагу до приватного життя, а відтак таке втручання 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) із боку приватних суб'єктів.

Серед рішень Європейського суду з прав людини, які мають безпосереднє відношення до права особи на захист персональних даних, можна виділити наступні:

- «Gaskin v. The United Kingdom» (заява № 10454/83, рішення від 07/07/1989) – Обмеження доступу особи до її персональних даних (документів щодо виховання дитини опікуном/прийомними батьками) з огляду на відсутність незалежного органу, який би розглядав клопотання щодо надання доступу. Порушення;
- «Leander v. Sweden» (заява № 9248/81) – Законність ведення таємного реєстру поліції та проведення перевірки особи за наявною у ньому інформацією перед зайняттям низки посад. Законність ведення реєстру та отримання доступу до нього. Контроль за веденням реєстру. Відсутність порушення;
- «M.S. v. Sweden» (заява № 34209/92, рішення від 27/08/1997) – Передача лікарнею медичної інформації про особу на запит державного органу. Відсутність порушення;
- «K.U. v. Finland» (заява № 2872/02, рішення від 02/12/2008);
- «Amann v. Switzerland» (заява № 27798/95, рішення від 16/02/2000) – Прослуховування телефонних розмов. За-

конодавча невизначеність повноважень щодо зберігання інформації про особу. Порушення;
- «Rotaru v. Romania» (заява № 28341/95, рішення від 04/05/2000) Законність ведення службою безпеки таємного реєстру. Відсутність законодавчих гарантій. Порушення;
- «I. v. Finland» (заява № 20511/03, рішення від 17/07/2008) – Відсутність обліку фактів щодо надання доступу до медичної документації заявниці, що призвело до неможливості встановлення особи, яка ймовірно поширила інформацію, що містилася у ній. Тягар доведення у справах щодо поширення персональних даних. Порушення;
- «K.H. and Others v. Slovakia» (заява № 32881/04, рішення від 06/11/2009) – Ненадання лікарнею заявникам копій їх медичної документації. Порушення;
- «L.H. v. Latvia» (заява № 52019/07, рішення від 29/04/2014) – Збір інформації контролюючим органом із метою оцінки якості наданої пацієнту медичної допомоги лікарнею. Відсутність легітимної мети збору персональних даних. Надмірний об'єм зібраної інформації. Неврахування інтересів пацієнта. Порушення;
- «M.K. v. France» (заява № 19522/09, рішення від 18/04/2013) – Ведення реєстру відбитків пальців. Принцип необхідності та пропорційності збору персональних даних. Порушення;
- «M.M. v. The United Kingdom» (заява № 24029/07, рішення від 13/11/2012);
- «Gardel v. France» (заява № 16428/05, рішення від 17/12/2009) – Ведення національними органами влади реєстру осіб, які вчинили злочини статевого характеру. Відсутність порушення;
- «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) – Законність підстав та порядку проведення негласного спостереження (перегляд кореспонденції, прослуховування розмов). Відсутність порушення;
- «Lenev v. Bulgaria» (заява № 41452/07, рішення від 04/12/2012) – Законність системи негласного спостереження. Порушення;

- «Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria» (заява № 62540/00, рішення від 28/06/2007) – Законність системи негласного спостереження. Порушення;
- «Klass and Others v. Germany» (рішення від 06/09/1978) – Законність прослуховування телефонних розмов. Порушення;
- «Z. v. Finland» (заява № 22009/93, рішення від 25/02/1997) – Недостатність строків, впродовж яких обмежувався доступ до рішення суду, що містив чутливу інформацію про заявницю. Порушення;
- «Avilkina and Others v. Russia» (заява № 1585/09, рішення від 06/06/2013) – Збір медичної інформації прокуратурою. Законодавча невизначеність повноважень щодо збору інформації про особу. Надмірний об'єм інформації, що збирається. Порушення;
- «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 та збереження зразків голосу. Порушення;
- «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 достатньо чіткої мети збору інформації, відсутність необхідності у зборі такого великого об'єму даних у порівнянні з отримуваними перевагами, неврахування індивідуальних обставин осіб, чиї дані зберігалися. Порушення;
- «Peck v. The United Kingdom» (заява № 44647/98, рішення від 28/01/2003) – Необхідність оприлюднення відеозапису, на якому видно заявника після того, як він намагався вчинити самогубство;
- «Mentzen v. Latvia» (заява № 71074, рішення від 07/12/2004);
- «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. Порушення;
– «Garnaga v. Ukraine» (заява № 20390/07, рішення від 16/05/2013) – Закріплена на законодавчому рівні неможливість змінити по батькові особи. Порушення;
– «Zaichenko v. Ukraine» (№ 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 чиїх діях вбачаються ознаки адміністративного правопорушення) в рамках провадження у справі про адміністративне правопорушення. Порушення.

Ключові положення вказаних рішень Європейського суду з прав людини лягли в основу прийнятої 28 січня 1981 р. Конвенції № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Цей документ став першим у цій сфері. У ньому вперше 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 положення вказаних документів дещо застаріли та потребують суттєвої модернізації. У зв'язку з цим Радою Європи було засновано ad hoc Комітет з питань захисту персональних даних, метою діяльності якого є розробка оновленого проекту Конвенції.

Разом з тим, після прийняття Конвенції Комітетом міністрів Ради Європи велася активна робота в напрямку роз'яснення порядку застосування її положень у секторах, де здійснюється обробка найбільш чутливих категорій персональних даних. Із цією метою Комітет міністрів прийняв низку рекомендацій. Ці документи мають прикладний характер і сприяють підтриманню положень Кон-

венції в актуальному стані, а також вказують, яким чином слід розуміти її положення в сучасних реаліях. Для того, щоб відповідати новим викликам у сфері захисту персональних даних, вказані рекомендації регулярно переглядаються та оновлюються.

Так, сюди належать Рекомендація № R (97) 5 Комітету міністрів державам-членам Ради Європи щодо захисту медичних даних, Рекомендація № R (91) 10 Комітету міністрів державам-членам Ради Європи щодо передачі третім сторонам персональних даних, що знаходяться у віданні державних органів, Рекомендація № R (89) 2 Комітету міністрів державам-членам Ради Європи про захист персональних даних, які використовуються для потреб працевлаштування, Рекомендація № R (87) 15 Комітету міністрів державам-членам Ради Європи щодо використання персональних даних у секторі поліції.

Сьогодні локомотивом розвитку законодавства 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) є найбільш сучасним документом, який встановлює достатньо детальні вимоги щодо того, як має бути організована система захисту персональних даних у державі.

Формально цей документ не є частиною українського законодавства. Однак, по-перше, він є ключовим у системі захисту персональних даних держав-членів Європейського Союзу, який є орієнтиром розвитку національної економічної, політичної та правової системи, і, по-друге, Закон України «Про захист персональних даних» базується фактично повністю на положеннях Директиви. Можна стверджувати, що якби не Директива, положення Закону було би вкрай важко правильно розуміти.

Так, низка положень Директиви недостатньо чітко/правильно сформульовані в Законі, тому для його правильного розуміння рекомендовано звертатися до відповідних положень Директиви.

ПРИКЛАД 1.

Закон України «Про захист персональних даних» (далі – Закон)

Стаття 11. Підстави для обробки персональних даних

1. Підставами для обробки персональних даних є:

(…) 2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; (…)

Для порівняння: Директива 95/46/ЄС

Article 7/ Стаття 7

Member States shall provide that personal data may be processed only if/ Держави-члени повинні забезпечити, щоб персональні дані оброблялися лише, якщо:

(…) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (…) / обробка є необхідною для виконання завдання, метою якого є задоволення суспільних інтересів, чи для виконання офіційних повноважень, якими наділений володілець чи третя сторона, якій передаються персональні дані.

Фактично Директива є рамковим документом, що встановлює лише мету, якої необхідно досягти. Це означає, що держави-члени володіють певною свободою розсуду щодо механізмів та порядку дотримання положень Директиви на національному рівні. Важливим при цьому є лише досягнення на національному рівні вказаної мети.

Наведені вище положення (Директиви та Закону) є по суті відповідниками, однак їх зміст суттєво відрізняється. Як показує практика, те, яким чином положення Директиви було викладено в Законі, призвело до неправильного розуміння підстав обробки персональних даних, відповідно до якого обробка персональних даних на підставі вказаного положення можлива лише, якщо існує норма закону, що безпосередньо санкціонує таку обробку. Однак, таке розуміння суперечить вказаному положенню Директиви (це питання розглядатиметься нижче).

Також положення Директиви передбачає, що «обробка є необхідною (…) для виконання офіційних повноважень, якими наділений володілець чи **третя сторона, якій передаються персональні дані**». Останнє взагалі не передбачається національним законодавством, хоч і є необхідним для належного функціонування системи захисту персональних даних.

Так, для того, щоб володілець мав право передати персональні дані третій особі, не лише у нього повинні бути підстави для передачі персональних даних. Третя особа для того, щоб їх законно отримати, також повинна мати підстави для їх обробки.

ПРИКЛАД 2.

У Директиві використовуються терміни «передача» персональних даних та «доступ» до них. Передача завжди стосується фактичного переходу персональних даних від одного володільця до іншого. В Директиві питання передачі окремо не розглядається, оскільки передача є по суті одним із видів обробки, а відтак всі правила щодо обробки автоматично застосовуються і до передачі. Поняття доступу використовується лише в контексті отримання суб'єктом відомостей про себе, які обробляються володільцем.

В Законі питання поширення (передачі) персональних даних розглядається в окремій статті, яка по суті повторює в спрощеному вигляді статтю 11 Закону. У статті 16 мова йде про доступ до персональних даних третіх осіб та самого суб'єкта. При цьому Закон не надає роз'яснення щодо різниці між поширенням персональних даних та наданням до них доступу третім особам.

По суті положення Закону та Директиви не суперечать одне одному. Однак, підхід визначений у Директиві є більш послідовним, доступним і надає правильне розуміння того, як повинні поширюватися персональні дані та за яких умов надається до них доступ.

Крім того, в рамках Європейського Союзу було прийнято цілу низку інших документів, що стосуються питання захисту персональних даних, а з 2012 р. триває процес реформування системи правового регулювання захисту персональних даних, що має завершитися прийняттям Регламенту з питань захисту персональних даних, який на відміну від Директиви, яка є рамковим документом, буде нормативно-правовим актом прямої дії.

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.

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, 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).

На виконання вказаного положення Конституції України, а також з метою імплементації Конвенції № 108 Ради Європи Верховною Радою України було прийнято Закон України «Про захист персональних даних», який закріплює основні зобов'язання володільців персональних даних, права суб'єктів персональних даних, основні підстави обробки персональних даних, порядок повідомлення наглядового органу про здійснення обробки, що становить особливий ризик для прав і свобод суб'єктів, принципи обмеження дії Закону, захисту персональних даних, повноваження наглядового органу та ін.. Законом передбачена, серед іншого, необхідність прийняття наглядовим органом у сфері захисту персональних даних, яким є станом на сьогодні Уповноважений Верховної Ради України з прав людини, низки підзаконних нормативно-правових актів у сфері захисту персональних даних.

У зв'язку з цим наказом Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02–14 було затверджено:

Типовий порядок обробки персональних даних;

Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних;

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.

Також Уповноваженим було підготовлено роз'яснення до вказаного документу.

Крім цього, положення Закону знаходять подальше роз'яснення в рішеннях судів, винесених за результатами розгляду адміністративних протоколів та приписів Уповноваженого, велика частина яких наводиться у даній праці в якості прикладів.

1.2. ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЇХ ВИДИ

Проблема термінологічного визначення та розуміння поняття «персональні дані» є однією із найскладніших при роботі в цій сфері. Саме у визначенні містяться межі та критерії віднесення тієї чи іншої інформації до цієї категорії. Аналізуючи ті визначення, які містяться в національних та міжнародних правових актах, слід зазначити, що в основному вони збігаються. Наприклад, в Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р., цей термін визначається як: «будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною».

На нашу думку, слід погодитися із визначенням, яке міститься в Законі, де персональні дані визначаються як: «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Це визначення є достатньо лаконічним і чітким та відповідає існуючим міжнародним підходам до розуміння цього поняття.

Ключовим у вищенаведеному визначенні також є поняття «ідентифікована особа». Ідентифікованою особа вважається, якщо її можна безпомилково виділити серед інших. 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.

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 відділені державного органу розвішується інформація щодо надання конкретним жителям району тих чи інших послуг 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 медичні особи та дані, 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 передаються іншій компанії для проведення наукових досліджень. В цьому випадку, провести ідентифікацію буде практично неможливо, через заходи із знеособлення.

Щодо класифікації видів персональних даних, слід зазначити, що такими актами, як Закон України «Про захист персональних даних» 2010 р. (ст. 7), Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» 1995 р. (ст. 8) та Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р. (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.

1.3. ПОНЯТТЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЇЇ ВИДИ

Відповідно до Закону України «Про захист персональних даних» 2010 р., 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 (базою даних, реєстром, каталогом, досьє тощо). Збір, реєстрація, накопичення чи будь-яка інша дія з боку володільця інформації навіть про одного суб'єкта персональних даних, у будь якій формі є обробкою відповідно до положень Закону.

Відповідно до усталеної практики Ради Європи та Європейського Союзу захист не є елементом обробки, оскільки не передбачає вчинення окремих дій над персональними даними. Використання зазвичай є елементом обробки, однак інколи (наприклад, у Німеччині) використання є окремою відносно обробки дією щодо персональних даних. При цьому, за жодних умов обробка не може бути елементом використання. Відповідно, «захист» персональних даних слід розглядати як окрему від їх «обробки» та «використання» дію, а «використання» – як один із елементів «обробки».

Водночас, слід зазначити, що в Законі України «Про захист персональних даних» 2010 р., разом із терміном «обробка» паралельно використовуються й інші терміни, зокрема «використання» та «захист». На жаль, Закон містить неправильне визначення вказаних термінів, що ускладнює його застосування. Відповідно до статей 2 та 10 Закону виникає така колізія:

Ст. 2 Закону
Обробка **включає** використання. Захист **не є** елементом обробки.

Ст. 10 Закону
Використання **включає** в себе обробку та захист.

Якщо говорити про види обробки персональних даних, то як специфічні категорії обробки варто виділити:

- обробку персональних даних у приватних цілях;
- обробку персональних даних у журналістських цілях;
- обробку персональних даних у творчих цілях.

Обробка персональних даних у приватних цілях відповідно до ст. 25 Закону України «Про захист персональних даних» 2010 р. не підпадає під його дію. Слід наголосити, приватний характер цілі передбачає здійснення обробки персональних даних для особистих, наприклад домашніх потреб, а не потреб особи загалом. Наприклад, ве-

дення особою телефонної книги є особистою потребою. Однак, якщо ця особа є власником бізнесу (наприклад, ресторанів чи магазинів) і збирає персональні дані клієнтів (ім'я, прізвище, по батькові і той же 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 1.

На веб-сайті однієї з місцевих газет було висвітлено інформацію про одного з ріелторів, щодо діяльності якого надходило безліч скарг від місцевих жителів. Інформацію було викладено у вигляді короткої вступної статті та великої кількості відгуків жителів міста. У вступній статті, серед іншого, висвітлено адресу вказаного ріелтора. Загалом висвітлення тієї інформації було актуальним та важливим питанням для жителів міста. Однак, розкриття адреси проживання вказаного ріелтора було надмірним і не обумовлювалося жодним інтересом, оскільки могло становити загрозу його життю та здоров'ю, не підсилюючи при цьому значення викладених матеріалів.

ПРИКЛАД 2.

На Інтернет-ресурсі одного із засобів масової інформації було викладено інформацію щодо осіб, які не з'явилися до військового комісаріату після вручення їм повістки, та осіб, які в певний період часу покинули місце розташування своєї військової частини. 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 війни є актуальною темою. Однак, оприлюднення персональних даних вказаних осіб жодним чином не сприяло висвітленню цієї тематики, достатньо було навести звичайну статистичну інформацію. Натомість абсолютно оче-

видно, що адміністрація сайту переслідувала мету стигматизації цих осіб як таких, що в тяжкий для держави час ухиляються від виконання свого військового обов'язку.

ПРИКЛАД 3.

У місцевій газеті в кримінальній рубриці було оприлюднено інформацію про те, що молодий хлопець внаслідок конфлікту з матір'ю вчинив самогубство. При цьому, висвітлювалися особисті дані матері та небіжчика. Суспільна вагомість такої інформації є дуже незначною, натомість втручання в особисте життя матері непомірно велике.

Відтак, усі вказані вище публікації є порушенням законодавства про захист персональних даних.

У цьому контексті слід також звернутися до практики Європейського суду з прав людини, яким неодноразово розглядалося питання дотримання балансу між правами особи на приватність та свободу вираження поглядів. Класичними у цьому відношенні є рішення Європейського суду з прав людини у справах «Фон Ганновер проти Німеччини», «Фон Ганновер проти Німеччини (№ 2)» та «Фон Ганновер проти Німеччини (№ 3)».

Серед інших термінів, пов'язаних із обробкою, слід виділити також «знеособлення персональних даних». Під знеособленням розуміємо 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 сканує медичну документацію, яка зберігається в архіві. Паралельно створюється окремий файл, що містить ідентифікаційні дані всіх осіб, яким належить вказана документація (пацієнтів). Ідентифікаційним даним пацієнтів та їх медичній документації присвоюється певний номер, після чого ці дані видаляються з медичної документації, а вказаний файл передається в МОЗ України. Таким чином, можливість дізнатися, кому належить документація, залишається. Проте, ні володілець, ні його працівники не в змозі цього зробити. Вказана медична документація була знеособлена.

1.4. ВОЛОДІЛЕЦЬ ПЕРСОНАЛЬНИХ ДАНИХ

Згідно з визначенням, закріпленим у Законі України «Про захист персональних даних» 2010 р., 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 Закону).

Таке розуміння терміну «володілець» є дещо застарілим, що, водночас, не робить його невірним. 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. Однак, ситуація складніша, коли мова йде про обробку персональних даних *на підставі закону*. У таких випадках мета обробки, склад даних та порядок їх обробки зазвичай визначено законодавством. Інколи законодавство встановлює, хто є володільцем/розпорядником.

ПРИКЛАД.

Порядок ведення реєстру хворих на туберкульоз, затверджений наказом МОЗ від 19.10.2012 року № 818, встановлює, що володільцем реєстру є протитуберкульозні заклади, а адміністратором – МОЗ. Проте, з огляду на повноваження адміністратора він фактично є співволодільцем, оскільки забезпечує надання доступу до реєстру, збереження та захист баз даних тощо.

Аналогічна ситуація з Положенням про електронний реєстр пацієнтів, затвердженим постановою КМУ від 6 червня 2012 року № 546, яким також визначено володільця і розпорядника.

При цьому, як видно з прикладу, наведеного вище, визначення того, хто є володільцем, як правило, надається законодавством, а не так, як вимагається, – законом (див. ст. 2 Закону). Разом з тим, часто ні законом, ні законодавством не встановлюється, хто є володільцем.

ПРИКЛАД.

Міністерство внутрішніх справ України затверджує порядок ведення дактилоскопічного обліку. Цим документом визначається мета такого обліку, склад даних, категорії суб'єктів, чиї дані обробляються та ін.. Однак саме Міністерство (а також його територіальні управління) безпосереднього доступу до вказаної інформації не має. Процедура отримання доступу визначена тим же наказом. Сама ж інформація зберігається в науково-дослідних експертно-криміналістичних центрах. Відтак, саме вони у цьому випадку повинні розглядатися в якості володільців.

Володільцем персональних даних у даному прикладі є той, у чиєму розпорядженні фактично перебувають персональні дані впродовж певного часу (крім випадків, коли мова йде про розпорядника – див. нижче).

У цьому зв'язку більш актуальним видається визначення володільця, викладене в оновленій версії Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р., яка ще перебуває на етапі розробки, згідно з яким володілець – це «фізична або юридична особа, орган державної влади чи будь-яка інша установа, яка самостійно чи разом з іншими має право приймати рішення щодо обробки персональних даних».

Також слід зазначити, що зазвичай володільцем є юридична чи фізична особа, однак можливі і винятки (див. приклади нижче).

ПРИКЛАД 1.

Якщо компанія є власником декількох юридичних осіб, кожна з яких веде базу даних власних працівників та клієнтів, саме ці юридичні особи будуть володільцями вказаних баз даних. Для передачі цих даних материнській компанії чи надання їй прямого доступу до них необхідно мати окрему підставу.

Підрозділи банку не є юридичними особами. Кожен з них користується доступом до єдиної клієнтської бази даних банку і лише центральний офіс приймає рішення щодо того, як оброблятимуться персональні дані клієнтів. Відтак, саме банк буде володільцем.

ПРИКЛАД 2.

Центр надання адміністративних послуг (далі – ЦНАП) є не відокремленою юридичною особою, а підрозділом виконавчого органу районної державної адміністрації. Незважаючи на це, відповідно до Закону України «Про адміністративні послуги» та Примірного регламенту центру надання адміністративних послуг, затвердженого постановою КМУ від 1 серпня 2013 р. № 588, ЦНАП має право зберігати документи/інформацію щодо осіб, яким було надано ті чи інші адміністративні послуги (тобто персональні дані вказаних осіб). Відтак, він має у своєму розпорядженні інформацію, до якої виконавчий орган районної державної адміністрації, який є юридичною особою, не має жодного відношення. Таким чином, фактично ЦНАП є володільцем.

Окрім того, слід зазначити, що:

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

ПРИКЛАД.

Дільничний інспектор міліції збирає та зберігає персональні дані осіб, які вчинили акт домашнього насильства. Крім цього, він передає таку інформацію до районного управління. Отже, кожен із них є володільцем вказаних персональних даних.

- якщо рівним доступом до однієї бази даних користуються два суб'єкти і кожен може приймати на свій розсуд рішення щодо обробки наявних у ній даних, їх слід розглядати як співволодільців;
- 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 вказаного об'єму даних. Поширеним прикладом такого виду обробки є функціонування міжвідомчих баз даних, порядок функціонування яких визначається спільними документами.

1.5. РОЗПОРЯДНИК ПЕРСОНАЛЬНИХ ДАНИХ

Відповідно до ст. 2 Закону України «Про захист персональних даних» 2010 р., розпорядник»ом 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 1.

Підприємства, що надають житлово-комунальні послуги, укладають договори з приватними компаніями, на підставі яких останні ведуть облік кількості та якості послуг, наданих підприємством спожива-

чам, 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.

ПРИКЛАД 2.

Банк укладає договір із приватною компанією, відповідно до якого остання зобов'язується вчинити за дорученням банку дії щодо повернення простроченої заборгованості низки боржників. Із цією метою банк передає реєстр боржників, що містить інформацію, необхідну для виконання договору. У такому випадку компанія діє (в тому числі обробляє персональні дані боржників) виключно в межах повноважень, наданих банком, і зобов'язується зберігати конфіденційність переданої банком інформації. Жодних нових повноважень у порівнянні з банком компанія не отримує. Така компанія буде розпорядником.

Таким чином, Закон встановлює ключові аспекти щодо поняття розпорядника та його відносин із володільцем, які однак не є достатніми та потребують суттєвого доповнення. Більш детально це питання розглядатиметься нижче, в частині, де мова йтиме про концепцію змін до національного законодавства у цій сфері.

1.6. ТРЕТІ ОСОБИ, ОДЕРЖУВАЧ ТА УПОВНОВАЖЕНИЙ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ

Відповідно до Закону України «Про захист персональних даних» 2010 р., одержувач персональних даних – це «фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа». Своєю чергою, третя особа – це будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України 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 одні-

єї 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 клієнтів 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 України «Про захист персональних даних» 2010 р., до складу суб'єктів, пов'язаних із відносинами щодо персональних даних, належить також Уповноважений Верховної Ради України 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.

ТЕМА 2. ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ.

2.1. ПОНЯТТЯ ТА ВИДИНИ ПРИНЦИПІВ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Обробка персональних даних ґрунтується на цілій низці принципів, які визначають основні правові засади її здійснення. Вказані принципи викладено у статті 5 Конвенції, статті 6 Директиви та статті 6 Закону. Під принципами розуміють правила, що повинні дотримуватися (за незначними виключеннями) будь-яким володільцем у ході здійснення будь-якої обробки.

Традиційно сюди належать такі принципи:

- ***законності та справедливості*** (англ. fairness, станом на сьогодні цей принцип частіше формулюється як принцип прозорості обробки персональних даних);
- ***легітимної мети***;

- ***адекватності, належності*** (відповідності) ***та пропорційності*** (ненадмірності) 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.

В Законі вказані принципи викладено в **статті 6**, відповідно до якої:

- Обробка персональних даних здійснюється для **конкретних і законних цілей**, визначених **за згодою суб'єкта персональних даних**, або у випадках, **передбачених законами України, у порядку, встановленому законодавством**.
- Обробка персональних даних здійснюється **відкрито і прозоро** зі застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.
- Персональні дані мають бути **точними, достовірними та оновлюватися в міру потреби**, визначеної метою їх обробки.
- Склад та зміст персональних даних мають бути **відповідними, адекватними та ненадмірними** стосовно визначеної мети їх обробки.
- **Персональні дані обробляються** 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.

Деколи до вказаних принципів додається також принцип *підзвітності*, згідно з яким кожен володілець повинен вживати всіх необхідних заходів із метою дотримання стандартів захисту персональних даних в ході їх обробки, а також бути здатним у будь-який момент надати наглядовому органу/суб'єкту персональних даних документи, які продемонструють, яких заходів було вжито[1]. В Законі цей принцип окремо не виділяється, однак він логічно випливає з його положень, зокрема з принципів відкритості та прозорості.

[1] Handbook on European Data Protection Law, підготований Агенцією Фундаментальних Прав Європейського Союзу, ст. 75–77.

Більшість інших положень вищезазначених правових актів є логічним продовженням, розвитком, деталізацією вказаних принципів і повинні розглядатися у їх світлі. На приклад, 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 фактично деталізацією принципу справедливості (англ. fairness) 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, серед іншого, принципу законності.

Слід зазначити, що вказані вище принципи обробки співпадають зі стандартами, виробленими в практиці Європейського суду з прав людини. Так, у своїх рішеннях ЄСПЛ неодноразово наголошував на тому, що обробка інформації щодо приватного життя особи входить у сферу статті 8 Конвенції про захист прав людини і основоположних свобод (див. рішення у справі «Ротару проти Румунії», заява № 28341/95, п. 43). Саме лише «зберігання органом влади інформації щодо приватного життя особи, становить втручання в права, гарантовані статтею 8 Конвенції, незалежно від того, як вказана інформація використовуватиметься в подальшому» (див. справи «Леандер проти Швеції» та «Копп проти Швейцарії»).

ПРИКЛАД.

«S. and Marper v. The United Kingdom» (заяви № 30562/04 і 30566/04, рішення від 04/12/2008)

66. Суд зазначає, що поняття приватного життя **є широким терміном, що не має вичерпного визначення**. Воно охоплює фізичну та психологічну цілісність особи (див. рішення у справі *Pretty v. the United Kingdom*, № 2346/02, п. 61). Також воно може охоплювати численні аспекти фізичної та соціальної ідентичності особи (див. рішення у справі *Mikulić v. Croatia*, № 53176/99, п. 53). Такі поняття, як наприклад, гендерна ідентифікація, ім'я, сексуальна орієнтація та статеве життя потрапляють у сферу, що захищається статтею 8 Конвенції. (див., наприклад, рішення у справах *Bensaid v. the United Kingdom*, № 44599/98, п. 47 та *Peck v. the United Kingdom*, № 44647/98, п. 57). Окрім імені особи, її чи його приватне життя може включати інші засоби особистої ідентифікації та зв'язку з сім'єю

(див. *mutatis mutandis* рішення у справі *Burghartz v. Switzerland* від 22 лютого 1994 року, п. 24 та у справі *Ünal Tekeli v. Turkey*, № 29865/96, п. 42). Важливим елементом приватного життя особи є інформація щодо стану її здоров'я (див. рішення у справі *Z v. Finland* від 25 лютого 1997, п. 71). Суд вважає, що сюди також належить інформація щодо етнічного походження особи (див. статтю 6 Конвенції про захист персональних даних, яка відносить персональні дані щодо расової приналежності до чутливої інформації про особу) (авт. – п. 41 рішення). Крім цього, стаття 8 захищає право на особистий розвиток та право встановлювати і розвивати відносини з іншими людьми та довколишнім світом (див., наприклад, ухвалу у справі *Friedl v. Austria* від 31 січня 1995 р., думка Комісії, п. 45). Також поняття приватного життя включає елементи права особи на власне зображення (див., наприклад, рішення у справі *Sciacca v. Italy*, заява № 50774/99, п. 29).

Для того, щоб таке втручання в права, гарантовані статтею 8 Конвенції, відповідало положенням цієї Конвенції, воно повинне: 1) базуватися на законі; 2) переслідувати одну з легітимних цілей, передбачених статтею 8; та 3) бути необхідним для досягнення такої цілі.

Не важко провести паралелі між принципами невтручання в право на повагу до приватності та принципами обробки персональних даних, викладених у Конвенції. Так, принципи справедливості та законності очевидно близькі вимозі Конвенції про те, що втручання повинне «базуватися на законі». Як втручання за Конвенцією, так і обробка повинні переслідувати легітимну мету та бути необхідними для її досягнення.

Інші принципи обробки персональних даних, передбачені Конвенцією (точності, справедливості, обмеженості строків, адекватності, належності (відповідності) та пропорційності), згадуються також і в практиці ЄСПЛ, однак не окремо, а в рамках вказаних критеріїв правомірного втручання в права, гарантовані статтею 8 Конвенції про захист прав людини і основоположних свобод. Наприклад, у справі «С. та Марпер проти Великобританії» необмеженість строку зберігання зразків ДНК, профілів ДНК та відбитків пальців працівниками правоохоронних органів стала однією з підстав для того, щоб констатувати, що втручання не було необхідним. Схожа ситуація у справі «М.К. проти Франції»[2], у якій невибірковий підхід до строків зберігання відбитків пальців в базі ОВС (відбитки вноси-

[2] «M.K. v. France» (заява № 19522/09, рішення від 18/04/2013).

лися до бази та зберігалися там 25 років, не враховуючи тяжкість злочину та чи було особу засуджено/виправдано, вік особи) розглядався ЄСПЛ як один із елементів порушення принципу необхідності/пропорційності. Законність втручання в практиці Європейського суду з прав людини передбачає, серед іншого, що положення законодавства, які регламентують порядок збору інформації про особу є доступними та чіткими (див. вище), що до певної міри відображає сутність принципу, відповідно до якого обробка повинна здійснюватися справедливо та прозоро.

Нижче, ці принципи буде розглянуто детальніше.

2.2. ЗАКОННІСТЬ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Цей принцип закріплено в п. «а» ч. 1 ст. 5 Конвенції, п. «а» ч. 1 ст. 6 Директиви, а також ст. 6 Закону.

Більш детально він тлумачиться у практиці Європейського суду з прав людини. Так, відповідно до ст. 8 Конвенції, втручання в гарантоване нею права можливе 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** у частині наслідків його застосування (див. рішення у справі «Аманн проти Швейцарії», заява № 28341/95, п. 48). Вимога щодо доступності зазвичай виконується, якщо той чи інший нормативно-правовий акт було оприлюднено (див. рішення у справі «Ротару проти Румунії», заява № 27798/95, п. 48). Щодо вимоги передбачуваності, то ЄСПЛ 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. 49).

В Україні загальні засади та принципи обробки персональних даних передбачено Законом. Його положення є рамковими та встановлюють загальні вимоги щодо того, яким чином повинна здійснюватися обробка персональних даних конкретними володільцями та яких правил при цьому дотримуватися. Лише обробка, що від-

повідає його положенням, розглядатиметься як така, що відповідає принципу законності.

При цьому зазвичай положень Закону недостатньо для того, щоб обробка була законною. У зв'язку з цим окремі його положення слід деталізувати в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних (ч. 1 ст. 6 Закону).

Загалом такі документи повинні по можливості визначати мету та підстави обробки персональних даних:

1) категорії суб'єктів персональних даних;
2) склад персональних даних;
3) порядок обробки персональних даних, а саме:
   - спосіб збору, накопичення персональних даних;
   - строк та умови зберігання персональних даних;
   - умови та процедуру зміни, видалення або знищення персональних даних;
   - умови та процедуру передачі персональних даних та перелік третіх осіб, яким можуть передаватися персональні дані;
   - порядок реалізації прав суб'єкта персональних даних;
4) організаційні та технічні заходи забезпечення захисту персональних даних;
5) процедуру збереження інформації про операції, пов'язані з обробкою персональних даних та доступом до них тощо.

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

ПРИКЛАД.

Справа «Ротару проти Румунії»[3].

У справі «Rotaru v. Romania» Служба розвідки Румунії (далі – СРР) володіла файлом, що містив персональні дані заявника. Серед іншого, там містилася інформація п'ятдесятилітньої давності про студентські роки заявника, навчання, участь у політичних організаціях – загалом загальнодоступна інформація. Заявник стверджував, що зберігання вказаної інформації СРР було незаконним (мова йшла про те, що на заявника в СРР було сформовано окрему «справу»). Європейський суд зазначив, що єдиною підставою була норма в законі, який регламентував порядок роботи СРР, згідно з якою СРР мала право збирати, зберігати та викорис-

[3] «Rotaru v. Romania" (заява № 28341/95, рішення від 04/05/2000).

товувати інформацію, що має значення для національної безпеки. З цих міркувань Суд вказав, що втручання мало підстави відповідно до національного законодавства (див. вище). Далі 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. Закон також визначав, що СРР отримувала право зберігати та використовувати архіви, отримані від попередніх служб розвідки. При цьому не було визначено, 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 СРР у цій частині. З огляду на зазначені факти Суд вказав, що законодавство, яке регламентувало втручання в права заявника (збереження щодо нього вказаної інформації СРР) не було достатньо передбачуваним. Відтак, втручання в його права не було законним і порушувало статтю 8 Конвенції.

2.3. ВИЗНАЧЕНІСТЬ МЕТИ

Відповідно до 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. 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.

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

З огляду на те, що Конвенція є частиною національного законодавства, положення Закону слід розглядати в її контексті.

Виходячи з цього, слід перш за все зазначити, що мета обробки повинна бути **легітимною**, тобто не повинна суперечити чинному законодавству.

Мета має бути **чітко сформульована**. Вказана ознака особливо важлива, оскільки є першочерговим 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 також він мав можливість контролювати їх обробку.

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 вимагатимуть внесення змін до закону чи модифікації умов згоди (більш детально про це мова йтиме нижче, в частині щодо адекватності, пропорційності та ненадмірності обробки).

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» заявника було затримано за крадіжку та відібрано відбитки пальців. У подальшому справу було закрито. Заявник звернувся до прокурора з вимогою видалити відбитки пальців, однак йому було відмовлено (на тій підставі, що це мало виключити його причетність до інших злочинів, вчинених третіми особами, якщо вони надумають «викрасти його ідентичність»). Суди залишили без змін рішення прокурора (в якості обґрунтування доцільності зберігання його відбитків було вказано на необхідність ведення якомога більшої та повнішої бази для порівняння, а також наявність гарантій конфіденційності інформації в базі). Суд, не розглядаючи питання законності втручан-

ня, вказав на наявність легітимної мети та перейшов до розгляду пропорційності втручання. У цьому зв'язку Суд зазначив, що цілі обробки відбитків пальців у вказаній базі даних, вказані прокуратурою та судами не вказувалися в законодавстві і фактично санкціонували зібрання відбитків всього населення, що було надмірним та непотрібним. Відбитки збираються не лише у справах щодо серйозних злочинів, а й щодо будь-яких найдрібніших злочинів.

Відбитки зберігалися незалежно від того, чи було особу в подальшому засуджено, що несло в собі ризик стигматизації (з особами, яких було виправдано (чи провадження, щодо яких було закрито), і на них поширюється презумпція невинуватості) поводяться як із засудженими). Ймовірність видалення відбитків за скаргою ілюзорна з огляду на мету – **накопичення якомога більшої кількості зразків для порівняння**. Усі відбитки зберігалися впродовж 25 років, що є надмірним терміном. Таким чином, держава, на думку Суду, вийшла за межі наданої їй свободи розсуду і не збалансувала інтереси особи зі суспільними.

Тому, втручання було непропорційним і таким, що не відповідає вимогам статті 8 Конвенції.

У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен мати окрему підставу.

ПРИКЛАД.

Компанія надає своїм клієнтам туристичні послуги та збирає з цією метою необхідні персональні дані. Підставою такої обробки є укладений між компанією та клієнтом договір, а метою – виконання відповідного договору. В подальшому компанія приймає рішення щодо використання (обробки) накопичених персональних даних клієнтів з метою здійснення цільового маркетингу (зокрема просування своїх послуг на ринку шляхом безпосереднього інформування про них кожного клієнта). Така мета не була передбачена початковим договором. Із цього моменту для того, щоб і надалі обробляти персональні дані клієнта (вже з іншою метою) компанія повинна знайти інші підстави для обробки його персональних даних (зазвичай підставою обробки буде необхідність реалізації законних інтересів (див. нижче розділ щодо підстав обробки).

У випадку, коли до компанії звернуться правоохоронні органи з вимогою надати інформацію щодо одного з клієнтів, яка необхідна для розслідування порушеної щодо нього кримінальної справи, компанія буде змушена передати таку інформацію (хоча така мета обробки не була передбачена договором з клієнтом). У такому випадку підставою передачі персональних даних клієнта буде необхідність виконання передбаченого законом обов'язку (див. розділ щодо підстав обробки нижче).

Разом з тим, законодавство та практика європейських держав свідчать про те, що не потрібно окремих підстав для подальшої обробки персональних даних у наукових, історичних та статистичних цілях.

Так, згідно з Директивою **за умови наявності достатніх гарантій** подальша обробка (авт. – зібраних до того в інших цілях) персональних даних в наукових, історичних та статистичних цілях є можливою. Для обробки персональних даних у вказаних цілях Директива дозволяє продовжувати строк їх зберігання (стаття 6 Директиви), а також обмежувати певні права особи в частині, що стосується обробки персональних даних, коли мова йде про подальшу обробку зібраних даних у наукових, статистичних та історичних цілях. Так, дозволяється не повідомляти суб'єкта персональних даних про обробку інформації про нього у вказаних цілях за умови забезпечення державою відповідних гарантій, а також якщо: 1) надання такого повідомлення становить непропорційний тягар чи є неможливим або 2) право обробки інформації чітко передбачено законом (стаття 11). Директивою дозволяється обмежувати право суб'єкта на доступ до інформації про нього та порядок обробки його персональних даних, а також право їх коригувати (статті 12–13).

Конвенція не дозволяє напряму автоматично обробляти персональні дані суб'єктів у наукових, історичних та статистичних цілях. Однак, у разі якщо така обробка здійснюється (з дотриманням усіх критеріїв законності такої обробки), Конвенція передбачає можливість встановлення законодавчих обмежень на права суб'єктів, визначені п.п. b, c та d ст. 8 Конвенції (право отримувати з розумними інтервалами відомості про те, чи здійснюється обробка, мати доступ до даних про себе, вимагати виправлення та знищення таких даних, звертатися до засобів правового захисту).

Такі положення Конвенції виглядають дещо застарілими, що пояснюється часом прийняття вказаного документу. Разом із тим, прийняті в подальшому на основі Конвенції рекомендації Комітету міністрів суттєво оновлюють її положення та наближають за змістом до Директиви.

Рекомендації КМ РЄ з цих питань[4] передбачають, що за загальним правилом персональні дані, зібрані для інших цілей, які пла-

[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.

нується використовувати в наукових чи статистичних цілях, повинні бути знеособленими шляхом видалення ідентифікуючих даних (тобто таких, що дають можливість ідентифікувати особу). Якщо є така можливість, ідентифікуючі дані повинні зберігатися окремо від решти даних[5].

Разом з тим, **за умови дотримання низки гарантій**, коли це необхідно для проведення відповідного статистичного чи наукового дослідження, ідентифікуючі дані можуть і не видалятися. Такі **гарантії** передбачають зокрема, що проведення дослідження можливе, якщо воно становить суттєвий публічний інтерес/санкціоноване уповноваженим суб'єктом та лише за умови, що: 1) суб'єкт персональних даних не висловлює очевидних заперечень, 2) незважаючи на розумні зусилля, зв'язуватися з суб'єктом з метою отримання його згоди було б непрактично й 3) інтереси проведення дослідження виправдовують вжиття таких заходів[6]. Персональні дані, зібрані в інших цілях, можуть використовуватися в цілях проведення статистичного дослідження, коли це необхідно: 1) для виконання завдання, що становить публічний інтерес, чи завдання що виконується з метою реалізації офіційних повноважень 2) з метою досягнення легітимних інтересів, які переслідуються володільцем, крім випадків, коли права та основоположні свободи суб'єктів персональних даних переважають такі інтереси.

В підсумку слід зазначити, що практика європейських держав є доволі одностайною у цьому напрямку та виходить з того, що наукові, статистичні (а відтак і історичні) дослідження слід проводити без використання ідентифікуючих даних. Коли ж це неможливо чи отримання законних підстав (наприклад, згоди особи на обробку її даних) становить надмірний тягар для володільця, дозволяється за умови дотримання низки гарантій використання ідентифікуючих даних у наукових, історичних чи статистичних цілях.

Така система є практичною та логічною, а тому повинна бути зразком для формування національного законодавства.

Проте, національне законодавство в цій частині є менш послідовним. Відповідно до ч. 8 ст. 6 Закону, «персональні дані обробля-

[5] П.п. 4.7, 8.1, 10.1, 11.1 Рекомендації КМ РЄ № R (97) 5 щодо захисту персональних даних, які збираються та обробляються в цілях статистики; п. 12.1 Рекомендації КМ РЄ № R (97) 18 щодо захисту медичних даних.

[6] П. 12.2.c Рекомендації КМ РЄ № R (97) 18 щодо захисту медичних даних.

ються 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. *Подальша обробка персональних даних у історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту*».

Крім того, відповідно до ч. 1 та 2 ст. 21 Закону, «про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом. *Повідомлення, зазначені у частині першій цієї статті, не здійснюються у разі: (...) 3) здійснення обробки персональних даних в історичних, статистичних чи наукових цілях; (...)*»

Вже згадувалося, що відповідно до 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.

Аналізуючи вказані положення Закону з урахуванням міжнародних документів, про які мова йшла вище, можна дійти до висновків про те, що наукові, історичні та статистичні цілі слід розглядати як ***сумісні*** в сенсі ч. 1 ст. 6 Закону. **Відтак, подальша обробка зібраних до того персональних даних в історичних, статистичних чи наукових цілях не потребує наявності окремої підстави**. Це можливо за умови «забезпечення їх належного захисту» (ч. 8 ст. 8 Закону)/»наявності достатніх гарантій» (ст. 6 Директиви, вказані вище Рекомендації). Приклади таких гарантій детально викладено у вищезазначених Рекомендаціях (див. вище).

Разом з тим, навіть якщо вважати, що історичні, статистичні чи наукові цілі є сумісними з будь-якою початковою метою, положення інших законів перешкоджають автоматичній обробці даних у вказаних цілях. Так, відповідно до ч. 2 ст. 40 Закону України «Про основи законодавства про охорону здоров'я», «при використанні інформації, що становить лікарську таємницю, в навчальному процесі, **науково-дослідній роботі**, в тому числі у випадках її публікації у спеціальній літературі, **повинна бути забезпечена анонімність пацієнта**». Це положення не містить жодних логічних у такій ситуації застережень чи виключень. Його логіка є зрозумілою з точки зору

захисту персональних даних, однак інколи такий категоричний підхід перешкоджає проведенню наукових досліджень.

Так, проведення досліджень у сфері медицини, написання наукових робіт у цій сфері зазвичай передбачає аналіз медичної інформації. В Україні така інформація фіксується в обліковій документації, яка після того, як у ній відпадає потреба, направляється до архіву. Облікова документація неодмінно містить ідентифікуючі дані пацієнта. Часто для того, щоб знеособити такий об'єм інформації чи відділити ідентифікуючі дані, необхідні надмірні зусилля. Крім цього, не виключені ситуації, коли персональні дані дійсно необхідні для проведення дослідження.

З цією метою видається необхідним деталізувати положення Закону в напрямку, який передбачено Директивою та відповідними Рекомендаціями КМ РЄ, зокрема передбачивши необхідні винятки, а також змінити аналогічним чином положення інших законів, зокрема у сфері охорони здоров'я.

До того часу видається доцільним із практичної точки зору вважати допустимою подальшу обробку персональних даних в історичних, статистичних чи наукових цілях за умови дотримання відповідних гарантій (див. вище) та у випадку, коли це дійсно необхідно для проведення дослідження.

ПРИКЛАД.

Працівниками Секретаріату Уповноваженого було проведено перевірку міської клінічної лікарні (далі – лікарня). В ході перегляду журналу вхідної-вихідної кореспонденції було виявлено лист Департаменту охорони здоров'я ОДА (далі – Департамент) з вимогою направити копії обмінних карт вагітних із результатами допологових обстежень в усіх випадках народження дітей із синдромом Дауна за період 2012–2013 років (далі – копії обмінних карт) та лист-відповідь лікарні, яким було направлено запитувану документацію. Із вказаних листів незрозуміло, якими були підстави та мета збору зазначеної інформації Департаментом.

Із метою вияснення зазначених питань працівниками Секретаріату Уповноваженого було проведено перевірку Департаменту. В ході перевірки було виявлено, що підставою направлення Департаментом запиту був отриманий ним лист МОЗ, із якого стало відомо, що вказані документи запитувалися з метою проведення дослідження, необхідного для удосконалення пренатальної діагностики медичними закладами. Згідно з вказівками, наданими в листі МОЗ, вказані документи слід було направити працівнику одного з медичних закладів (далі – дослідник), який спеціалізувався на вказаних питаннях. Однак, Уповноважений отримав

інформацію, яка свідчила, що копії обмінних карт було направлено також в МОЗ.

На думку Уповноваженого, вказані дії свідчили про наявність у діях МОЗ, Департаменту та лікарні низки порушень законодавства про захист персональних даних.

Так, МОЗ має право згідно з чинним на той час Положенням про МОЗ України, затвердженим Указом Президента України від 13 квітня 2011 року № 467/2011, організовувати наукові дослідження. За обставин даної справи вказане наукове дослідження повинне було проводитися дослідником. Ні Департамент, ні МОЗ не були задіяні в проведенні вказаного дослідження. Тому, направлення їм копій обмінних карт, що містять чутливу інформацію про стан здоров'я вагітних (їх персональні дані) не було необхідним та порушувало частину шосту статті 6 Закону, відповідно до якої «склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки».

Разом із тим такі дії (поширення персональних даних Департаменту та МОЗ) не можна вважати абсолютно незаконними.

Так, відповідно до п. 3 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*.

Відповідно до ч. 2 ст. 7 Закону допускається обробка даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних, ***якщо вона необхідна в цілях охорони здоров'я**, (...) за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю*.

Спочатку інформація про вагітних збиралася з метою надання медичної допомоги. В подальшому її було передано для проведення наукового дослідження, необхідного для підвищення якості надання медичної допомоги. Відтак, обидві цілі охоплюються поняттям «охорона здоров'я» у світлі статті 7 Закону. В силу цього подальша мета обробки не може вважатися несумісною з попередньою в сенсі статті 6 Закону. На всіх осіб, які отримували копії обмінних карт, поширювалося законодавство про лікарську таємницю. Вказані гарантії відповідають здебільшого тим, що передбачені положеннями статті 7 Закону. Крім того, допустимість подальшої обробки персональних даних щодо стану здоров'я особи в наукових цілях передбачена в Рекомендації КМ РЄ № R (97) 5 щодо захисту медичних даних.

Крім цього, з огляду на отримані коментарі МОЗ України проведення вказаного дослідження не потребувало використання особистих (іден-

тифікуючих) даних пацієнтів (імені, прізвища та по батькові). Для проведення дослідження необхідною була лише медична інформація, що містилася в копіях обмінних карт. Також 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 і копії обмінних карт було направлено разом із ідентифікуючими даними суб'єктів (вагітних). Такі дії лікарні становили порушення ч. 6 ст. 6 Закону, відповідно до якої «склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки».

У зв'язку з цим Уповноваженим було внесено припис вказаним установам (МОЗ та Департаменту) щодо знеособлення/видалення отриманих копій обмінних карт та вжиття практичних заходів щодо недопущення таких порушень у майбутньому.

Слід зазначити, передача персональних даних медичним закладом Департаменту була обумовлена іншим порушенням законодавства про захист персональних даних. Так, запит, направлений Департаментом до лікарні, був такого змісту:

«На виконання доручення МОЗ України (лист від _____ № _____) департамент ОЗ ОДА зобов'язує Вас надати завірені в установленому порядку копії індивідуальних карт вагітних із результатами допологових обстежень в усіх випадках народження дітей із синдромом Дауна за період 2012–2013 років. Термін виконання _____».

Відповідно до частин першої, третьої та четвертої статті 16 Закону, **порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних**, наданої володільцю персональних даних на обробку цих даних, **або відповідно до вимог закону**. Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу (далі – запит) до персональних даних володільцю персональних даних. У запиті зазначаються: (...) 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**.

З огляду на зазначені положення Закону володілець персональних даних має право їх поширювати лише за наявності законних підстав (згоди або закону), особливо, коли персональні дані поширюються з метою іншою, ніж та, з якою вони збиралися та оброблялися володільцем. Із метою дотримання вказаних положень, надаючи доступ до інформації, він повинен переконатися у тому, що третя сторона, якій надається такий

доступ, має на нього право. Для цього третя сторона повинна вказати підстави та мету отримання доступу до персональних даних у запиті.

У цій справі запит Департаменту було складено у наказовій формі без жодного пояснення щодо наявності в Департаменту підстав отримання доступу до запитуваної інформації чи мети, з якою вона запитується. Це, своєю чергою, призвело до того, що лікарня не могла надати оцінку щодо адекватності та пропорційності запитуваних персональних даних (про що мова йшла вище). За таких обставин лікарні слід було однозначно відмовити в задоволенні запиту Департаменту. Натомість факт надання такої інформації свідчить про порушення лікарнею вказаних вище положень статті 16 Закону. У зв'язку з цим керівництву лікарні було направлено роз'яснення щодо необхідності ретельного дотримання положень Закону.

Порушення вказаного положення необов'язково свідчить про незаконну обробку (доступ/поширення) персональних даних, що є підставою для притягнення до адміністративної відповідальності за частиною четвертою статті 188–39 КУпАП. Так, якщо в ході перевірки буде встановлено, що надання доступу мало законні підстави, воно не буде розглядатися в якості незаконного.

Також видається доцільним проведення автоматизації обробки медичної інформації, яка забезпечила би можливість безперешкодного відділення ідентифікуючих даних від решти медичної інформації. Створення електронної бази пацієнтів повинно базуватися на законі, у якому (а також НПА, виданих на його виконання) повинно бути детально викладено порядок обробки медичних даних пацієнтів (див. вище положення щодо принципу законності). Адміністрування такого реєстру має здійснюватися або державним органом, або спеціально для цього створеним державним підприємством.

2.4. АДЕКВАТНІСТЬ, ВІДПОВІДНІСТЬ ТА НЕНАДМІРНІСТЬ

У практиці Європейського суду з прав людини цей принцип сформульовано як принцип необхідності/пропорційності (див. принцип законності вище).

На перший погляд все видається зрозумілим, однак на практиці дотримання вказаного принципу перебуває на доволі низькому рівні. Відповідно до цього принципу склад та зміст персональних даних, що обробляються володільцем, а також спосіб їх обробки повинні відповідати легітимній меті їх обробки. Тобто, по-перше, об-

роблятися повинні виключно ті дані, обробка яких необхідна для досягнення мети (відповідність та ненадмірність даних – див. Приклад 1 нижче), і, по-друге, навіть якщо певні дані і є необхідними для досягнення мети, їх обробка буде незаконною, якщо її можна досягти і не здійснюючи обробки вказаних даних (адекватність – див. Приклад 2 нижче).

ПРИКЛАД 1.

У середній школі здійснюється обробка персональних даних школярів, а також персональних даних батьків. Підставами такої обробки є, серед іншого, Закони України «Про освіту», «Про загальну середню освіту» та ін.. Метою обробки персональних даних школярів є забезпечення їх права на загальну середню освіту. Реалізація вказаного права потребує обробки низки персональних даних школярів – особистих, медичних даних, даних щодо характеру, розвитку особистості тощо. Разом з тим велика кількість облікової документації, що ведеться школами, передбачає збір інформації щодо національності школярів. Обробка вказаних даних насправді не потрібна для реалізації ними свого права на освіту. Більше того, збір такої інформації може призвести до дискримінації тих чи інших категорій учнів. Відтак, обробка таких персональних даних про учнів буде непропорційною та невідповідною.

ПРИКЛАД 2.

Запровадження роботодавцями процедури ідентифікації персоналу з використанням відбитків пальців є однією з актуальних тем звернень громадян до Уповноваженого. Відцифровані відбитки пальців повинні у такому випадку зберігатися в окремому реєстрі володільця. Метою обробки було забезпечення реалізації обов'язків роботодавця, а саме підтримання трудової дисципліни та створення належних умов праці, забезпечення пропускного режиму на підприємстві. Заявники скаржаться на примусовий характер впровадження таких систем, які супроводжуються погрозами з боку роботодавців звільнити тих працівників, хто не погоджується надати відбитки пальців.

У цьому зв'язку слід зазначити, що згідно із визначенням терміну «біометричні дані», що міститься в Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» відцифровані відбитки пальців рук є біометричними даними.

Частиною 1 статті 7 Закону визначено біометричні дані як такі, обробка яких дозволяється лише у чітко визначених цим законом випадках. Зокрема, така обробка дозволена у разі необхідності здійснення володільцем персональних даних прав та виконання обов'язків у сфері трудових правовідносин відповідно до закону зі забезпеченням відповідного захисту (див. вище). Тобто, право адміністрації підприємства на збір та

використання біометричних даних, зокрема відбитків пальців, має бути визначено законом.

Якщо такого права не передбачено актами законодавства, що регулюють діяльність підприємства, а також якщо така обробка не обумовлена іншими підставами, визначеними статтею 7 Закону, обробка біометричних даних, зокрема відбитків пальців, може здійснюватися лише за умови надання працівниками на це окремої згоди.

У цьому зв'язку важливо звернути увагу на таке:

1. Надання згоди на обробку 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 чи електронній формі. Згода на обробку персональних даних має бути свідомим рішенням особи, яке вона приймає добровільно, без примусу і погроз (зокрема погрози звільнення).

2. За певних умов навіть обробка персональних даних, які використовуються для досягнення мети, може становити порушення, якщо цієї ж мети можливо було досягнути без їх обробки.

Окремо слід зазначити, що обробка персональних даних, на яку особа дає згоду, також повинна бути пропорційною меті обробки. **Навіть, якщо особа надала згоду на обробку персональних даних, які по своїй суті непотрібні для досягнення поставленої мети обробки, така обробка розглядатиметься як непропорційна та становитиме порушення законодавства про захист персональних даних**.

Так, за певних умов використання відбитків пальців дійсно переслідує вказану мету (підтримання трудової дисципліни та створення належних умов праці, забезпечення пропускного режиму на підприємстві), однак її досягнення можливе й іншими шляхами (введення системи магнітних карток, покладення на охорону підприємства обов'язків щодо ведення обліку робочого часу працівників та інше), які тягнуть за собою менший ступінь втручання в права особи на захист персональних даних. Це стосується, зокрема роботодавців, які не ведуть діяльності, яка потребує таких заходів безпеки. За таких умов використання біометричних даних особи не буде необхідним (адекватним, відповідним, ненадмірним).

3. Разом із тим за певних умов з огляду на важливість/небезпечність/вартість виробничих та інших процесів може бути доцільним використання біометричних замків (а відтак і даних) за згодою працівників.

У цьому зв'язку слід наголосити на важливості розмежування процедур ідентифікації та верифікації в ході обробки біометричних даних із метою реалізації трудових відносин.

Ідентифікація передбачає порівняння біометричних даних особи з даними, що зберігаються в базі біометричних даних володільця, з метою вирізнення конкретної особи з поміж інших.

У же той час метою верифікації є недопущення використання, наприклад, документів однієї людини іншою. Така процедура проводиться на

підставі даних, що міститься у відповідному документі, зокрема, в безконтактному електронному носії, який має бути складовою частиною документа, і не передбачає співставлення з даними окремої загальної бази, а безпосередньо з даними суб'єкта персональних даних.

Останній спосіб використання біометричних даних у сфері трудових відносин є найбільш прийнятним із точки зору захисту персональних даних. Адже збереження біометричних даних на локальному пристрої не потребує ведення володільцем бази біометричних даних працівників, а тому значно зменшує ризики несанкціонованого доступу до них або їх незаконного використання.

Разом із тим, необхідно ще раз підкреслити, що незалежно від способу та мети використання біометричних даних, їх обробка роботодавцями може здійснюватися лише на підставі добровільної, поінформованої згоди суб'єкта персональних даних. Ненадання такої згоди не може негативно позначатися на правах людини, тим більше обмежувати право особи на працю, гарантоване статтею 43 Конституції України.

Вказаний принцип повинен пронизувати будь-який процес обробки персональних даних незалежно від підстав здійснення такої обробки. Так, у прикладі, наведеному вище, вказувалося, що навіть у разі згоди особи на обробку персональних даних, така обробка є непропорційною відповідно до мети, вказаної володільцем.

Якщо обробка персональних даних здійснюється з метою виконання повноважень державного органу, 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, які обробляються. Оскільки не завжди можливо передбачити оптимальний склад даних, що необхідні для виконання повноважень державного органу, в ході їх обробки необхідно **враховувати індивідуальну ситуацію заявника, зокрема шляхом детального аналізу його звернень щодо припинення обробки, зміни чи виправлення його персональних даних**. Таким же чином повинні бути побудовані нормативно-правові акти, на підставі яких здійснюється обробка персональних даних.

ПРИКЛАД.

Справа «Гардель проти Франції»[7]. 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 встановив, що функціонування реєстру чітко передбачалося національним законодавством, яке детально регламентувало порядок його ведення, а відтак було законним. Збір викладеної у реєстрі інформації переслідував легітимну мету – запобігання вчиненню злочинів, захист чутливих категорій населення (дітей) та реінтеграція тих, хто вчинив злочин. Крім цього, Суд наголосив, що ведення реєстру було **необхідним та пропорційним у світлі вказаної мети** та супроводжувалося відповідними гарантіями захисту від порушення прав суб'єктів, оскільки:

- в реєстр вносилася інформація лише щодо осіб засуджених до покарання, що передбачало позбавлення волі на строк більше, ніж 1 рік;
- особа повідомлялася про внесення інформації про неї до реєстру та наслідки таких дій;
- строк зберігання інформації у реєстрі був обмеженим до 20–30 років залежно від тяжкості злочину;
- **в разі необхідності строк міг бути переглянутий прокурором до його завершення (з огляду на вік особи, плин часу, зміну особистості, життєвих обставин та ін.) і таке рішення могло бути оскаржене до суду**;
- можливі реципієнти інформації чітко визначені, як і мета отримання доступу та випадки, в яких вони можуть отримувати інформацію з реєстру;
- всі реципієнти були зв'язані зобов'язанням конфіденційності.

Відтак Суд констатував відсутність порушення прав заявника у вказаній справі.

Якщо обробка здійснюється з метою виконання обов'язку, передбаченого законом (наприклад, приватні володільці зобов'язані у випадках та в порядку, визначених законодавством, надавати інформацію за запитами правоохоронних, податкових та інших органів), приватні 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. Якщо ж склад таких даних визначено законодавством, як це часто трапляється, саме воно повинно, як і у випадку вище, враховувати дотримання принципу необхідності.

[7] «Gardel v. France» (заява № 16428/05, рішення від 17/12/2009).

Окремо слід зробити додаткові (до тих, що наводилися у прикладі щодо використання біометричних даних вище) застереження щодо застосування вказаного принципу в ході обробки персональних даних на підставі згоди особи (до певної міри це актуально і для договору). Так, доволі частими є ситуації, коли в особи береться «необмежена згода на обробку персональних даних» (тобто, санкціонується обробка необмеженої кількості даних та вчинення над ними будь-яких дій, пов'язаних з обробкою, як наприклад передача невизначеному колу суб'єктів), «безвідклична згода», а також коли особа надає згоду на обробку даних, що насправді непотрібні для досягнення задекларованої мети обробки.

Слід зазначити, що навіть якщо особа свідомо надасть згоду на таку обробку, вона не може бути законною, оскільки не відповідає вказаному вище принципу. В протилежному випадку це може потягти за собою зловживання вказаною підставою для обробки персональних даних, коли отримання особою тієї чи іншої послуги, яка має для неї суттєве значення, обумовлюватиметься наданням нею згоди на обробку непропорційно великого об'єму даних (наприклад під час підписання кредитного чи іншого договору).

2.5. 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. Крім того, вказане зобов'язання нерозривно пов'язане з правом суб'єкта персональних даних звертатися до володільця з вимогою виправити його персональні дані, якщо вони не відповідають дійсності, або привести їх в актуальний стан.

При цьому допускаються певні відступи від вказаного принципу в залежності від того, про яку сферу діяльності йде мова. Видається очевидним, що не вся інформація, яка обробляється деякими володільцями є на сто відсотків достовірною. Так, лікарі не завжди можуть гарантувати стопроцентну правильність діагнозу, а працівники правоохоронних органів – інформації щодо причетності особи до вчинення того чи іншого злочину.

В таких випадках важливо, по-перше, вживати в розумних межах всіх необхідних заходів для того, щоб зробити інформацію більш достовірною, а, по-друге, відділяти більш достовірну інформацію від менш достовірної.

2.6. СПРАВЕДЛИВІСТЬ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ (АНГЛ. PRINCIPLE OF FAIR PROCESSING)

Вказаний принцип закріплено як у Конвенції та Директиві, так і у Законі. Відповідно до п. «а» ст. 5 Конвенції персональні дані обробляються законно та справедливо. Аналогічне положення міститься і в статті 6 Директиви.

У національному законодавстві цей принцип викладено у п. 2 ч. 1 ст. 6 Закону, де мова йде про те, що «обробка персональних даних здійснюється **відкрито і прозоро** зі 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 та які дані обробляються, а також мати певні можливості щодо контролю обробки.

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

1) інформування суб'єкта персональних даних щодо обробки його персональних даних. Це зобов'язання передбачає обов'язок володільця автоматично надавати суб'єкту певну інформацію про обробку його персональних даних. Дане правило деталізується в інших положеннях Закону, а саме – п.п. 1, 2 ч. 2 ст. 8 та ч. 2 ст. 12 Закону. В Директиві схожі положення містяться у ст.ст. 10 та 11. У Конвенції окремої статті, присвяченої цьому питанню немає, однак вона включена в проект модернізованої Конвенції (стаття 7bis)[8]. Вказані поло-

[8] 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.

ження 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 логічно випливає право суб'єкта на виправлення, видалення та блокування його персональних даних у разі порушення якогось із зазначених вище принципів. У Конвенції ці права закріплено в статті 8, а в Директиві – статті 12. У Законі ці права передбачено пунктах 3, 4, 5 та 6 частини другої ст. 8, частини шостої ст. 16, статтях 20 та 21 Закону.
3) право суб'єкта направляти заперечення проти обробки його персональних даних із посиланням на вагомі та легітимні особисті обставини, право суб'єкта заперечити проти автоматизованого індивідуального рішення щодо нього та проти обробки персональних даних із метою здійснення цільового маркетингу. Вказані права чітко викладено в Директиві (стаття 15), однак у Конвенції відсутні. В Законі ці права викладено в загальних рисах у пунктах 5, 12 та 13 частини другої статті 8 Закону.
4) повідомлення наглядового органу у визначених законом випадках про обробку персональних даних та оприлюднення останнім такої інформації.

Наразі слід зазначити, що вказаний принцип було не в повній мірі імплементовано в національне законодавство. Положення Конвенції є надто загальними в частині зазначеного принципу та не відповідають вимогам сучасності. Автори Закону очевидно намагалися врахувати у ньому більш сучасні положення окремих Рекомендацій КМ РЄ та Директиви. Більшість положень вказаних документів у тій чи іншій мірі знайшли своє відображення в Законі, однак якість викладу є недостатньою. Велика кількість його положень у цій частині є надто заплутаними, стислими та незавершеними.

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

ТЕМА 3. ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. 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. 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 через призму положень статті 7 Директиви, оскільки, як зазначалося вище, вона (стаття 11 Закону) є безпосереднім результатом їх імплементації.

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**
– згода суб'єкта персональних даних на обробку його персональних даних (п. 1 ч. 1); – 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 (п. 3 ч. 1).	– дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень (п. 2 ч. 1); – захист життєво важливих інтересів суб'єкта персональних даних (п. 4 ч. 1); – необхідність виконання обов'язку володільця персональних даних, який передбачений законом (п. 5 ч. 1); – 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 (п. 6 ч. 1).

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. Разом з тим обробка медичними закладами інформації щодо стану здоров'я здійснюється у зв'язку з необхідністю виконання ними передбаченого законом обов'язку. Обробка чутливої інформації для виконання завдань оперативно-розшукової діяльності здійснюється правоохоронними органами у зв'язку з необхідністю виконання ними визначених законом повноважень.

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 п.п. 2, 4, 5 та 6 ч. 1 ст. 11 Закону. Остання виступає по суті протилежністю обробки, що базується на підставі згоди.

3.2. СТАТУС ПЕРСОНАЛЬНИХ ДАНИХ. ПЕРСОНАЛЬНІ ДАНІ ТА КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ

Виходячи із вказаних вище положень, доцільним видається розглянути питання щодо співвідношення поняття «персональні дані» та «конфіденційна інформація».

Відповідно до ст. 32 Конституції, не допускається збирання, зберігання, використання та поширення **конфіденційної інформації про особу** без її згоди, крім випадків, визначених законом, і лише

в інтересах національної безпеки, економічного добробуту та прав людини. Із вказаного положення випливає, що інформація про особу (персональні дані) може бути як конфіденційною, так і не належати до неї.

Відповідно до ст. 20 Закону України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Одним із видів інформації з обмеженим доступом є конфіденційна інформація. Конфіденційна інформація відповідно до ст. 21 Закону України «Про інформацію» може поширюватися за **бажанням (згодою)** відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а **також в інших випадках, визначених законом**.

Виходячи з цього, якщо персональні дані (всі чи окремі категорії) не охоплюються поняттям конфіденційної інформації, вони повинні розглядатися як відкрита інформація, а відтак можуть оброблятися фактично без обмежень. Ті ж персональні дані, що належать до конфіденційної інформації, можуть оброблятися лише за згодою суб'єкта або на підставі закону.

Однак, законодавчі положення щодо віднесення персональних даних до конфіденційної інформації є суперечливими.

Відповідно до ст. 21 Закону України «Про інформацію» **конфіденційною є інформація про фізичну особу**, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. При цьому, відповідно до частини 1 статті 11 того ж Закону, **інформація про особу є персональними даними**.

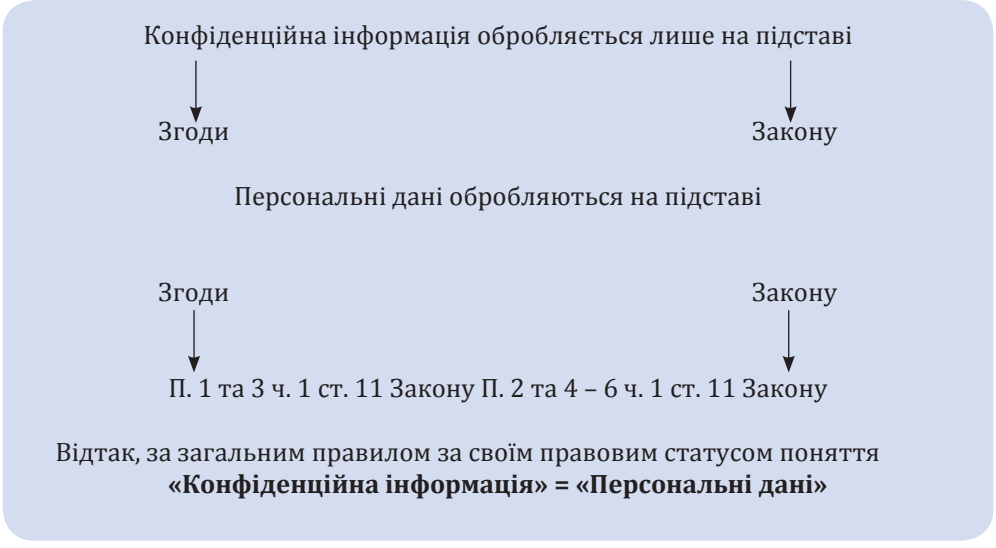
Відповідно до частини 2 статті 5 Закону України «Про захист персональних даних» **персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою**. Це положення створює фактичну презумпцію відкритості персональних даних.

Разом з тим статтею 11 Закону визначено вичерпний перелік підстав обробки персональних даних (і в тому числі їх поширення) (див. вище). Цей перелік є результатом імплементації положень Директиви і становить загальноприйнятий стандарт того, за яких умов дозволяється обробляти персональні дані. Тому саме зі статті 11 Закону слід виходити, вирішуючи питання щодо підстав обробки персональних даних.

Слід зазначити, концепція конфіденційної інформації носить дещо застарілий характер і є пережитком, характерним для держав пострадянського простору. Тривалий час така концепція передбачала, що сам факт віднесення законом інформації до конфіденційної незалежно від її характеру передбачав певне обмеження її обробки. Ситуація змінилася з прийняттям Закону України «Про захист персональних даних» та «Про доступ до публічної інформації». Вказані закони побудовано на абсолютно інших та нехарактерних до того для правової системи нашої держави концепціях, запозичених у Ради Європи, Європейського Союзу та практики Європейського суду з прав людини. Очевидно, що вони є більш гнучкими та пристосованими до сучасних реалій.

При цьому поняття «конфіденційна інформація про особу» згадується в Конституції, тому важливо визначитися зі співвідношенням понять персональних даних (як інформація про особу) та конфіденційної інформації.

Вище вже зазначалося, що підстави обробки персональних даних, вказані у статті 11 Закону, умовно можна розділити на дві групи, залежно від того, чи вони базуються на підставі згоди чи закону. Відтак можна дійти висновку, що персональні дані, як і конфіденційна інформація, можуть оброблятися лише за наявності згоди особи або на підставі закону. Тому логічним видається ототожнення понять персональних даних та конфіденційної інформації.



Разом з тим слід визнати, що станом на сьогодні шляхом віднесення персональних даних до конфіденційної інформації намагаються часто неправомірно закрити до них доступ. У цьому зв'язку слід зазначити, що незалежно від статусу персональних даних та їх приналежності до конфіденційної інформації, їх обробка здійснюється виключно на підставах, передбачених статтею 11 Закону, які є достатньо гнучкими (за умови внесення необхідних змін із метою приведення їх до повної відповідності положенням Директиви) та враховують усі можливі ситуації, коли виникає потреба в обробці персональних даних.

При цьому стаття 5 Закону та низка інших положень законодавства, як це і вимагається статтею 32 Конституції (яка, про що мова йшла вище, розділяє інформацію про особу на конфіденційну та відкриту), визначають категорії персональних даних, що не належать до конфіденційної інформації:

- персональні дані, що стосуються здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень;
- персональні дані, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, крім відомостей, зазначених Законом України «Про засади запобігання і протидії корупції»;
- інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна.

Така інформація є дійсно відкритою і кожна зацікавлена особа має право її знати. Ці положення узгоджуються із Законом. Так, як зазначалося вище, персональні дані обробляються за згодою особи або на підставі закону. У цьому випадку закон надає право обробляти визначені категорії персональних даних (див. вище).

Таке розуміння видається логічним, однак воно чітко не закріплене в національному законодавстві.

Тому видається доцільним внести зміни до Закону, а саме:

Варіант 1: видалити перше речення частини 2 статті 5 та прямо не вирішувати на законодавчому рівні питання співвідношення понять «персональні дані» та «конфіденційна інформація». Це непогане вирішення питання, оскільки поняття «конфіденційної інформації» є штучним та практично не впливає на те, чи оброблятимуться персональні дані; або

Варіант 2: викласти перше речення частини 2 статті 5 у такій редакції: «Персональні дані є конфіденційною інформацією та обробляються виключно на підставах, передбачених статтею 11 цього Закону».

При цьому слід акцентувати на неприпустимості підходу, закріпленого у вказаному положення статті 5 Закону (**персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою**). Із нього випливає, що персональні дані, які не є конфіденційною інформацією (а таких багато), є відкритою інформацією, при цьому немає чіткого посилання на статтю 11 Закону, яка є єдино правильним джерелом обробки персональних даних.

3.3. ОСНОВНІ ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Згода

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).

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

- добровільність;
- поінформованість;
- зовнішня форма, що дає змогу зробити висновок про надання згоди.

Добровільність згоди проявляється у відсутності прямого чи опосередкованого примусу при її наданні. За загальним правилом суб'єкт персональних даних має право самостійно вирішувати питання щодо того, чи давати згоду на обробку своїх персональних даних. Це підтверджується і тим, що 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.

Щодо прямого примусу, то тут все більш-менш зрозуміло – згода не може бути добровільною, якщо надавалася під тиском із боку представників володільця чи інших осіб. Якщо мова йде про опосередкований примус, мається на увазі ситуація, коли отримання особою тієї чи іншої життєво важливої послуги, чи реалізація тих чи інших прав ставиться в залежність від надання нею згоди на обробку

персональних даних. Зазвичай таке трапляється у випадках нерівності між суб'єктом та володільцем, зокрема залежності суб'єкта від володільця (зазвичай так і буває, оскільки суб'єкт звертається до володільця за тими чи іншими послугами). Вказана ситуація потребує більш детального висвітлення, оскільки є доволі поширеною в українському суспільстві.

Наприклад, впродовж тривалого часу особа не могла зареєструвати права на нерухоме майно, отримати диплом про закінчення школи чи ВУЗу, соціальну допомогу, адміністративну послугу в ЦНАП, а інколи і медичну допомогу, не надавши перед цим згоду на обробку персональних даних (вказаний перелік таких ситуації не є вичерпними і проблема досі залишається актуальною). Таким чином, особа ставиться у ситуацію, коли відмовившись від надання згоди, втрачає можливість реалізувати ті чи інші інколи життєво важливі права. Відтак, порушується принцип добровільності згоди.

Поінформованість передбачає, що 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).

Закон не передбачає форми надання такої інформації, однак очевидно, що, по-перше, володілець повинен за будь-яких умов мати можливість підтвердити факт надання такої інформації особі, оскільки в протилежному випадку це буде розглядатися як порушення статті 12 Закону, і, по-друге, така інформація повинна бути надана в доступному вигляді.

Наприклад, інформація не буде вважатися доступною, якщо надана у дуже складному вигляді, як це наприклад часто трапляється у мережі Інтернет, коли особі пропонується ознайомитися з умовами надміру великого та складного договору чи іншого документу, що може забрати непропорційно багато часу в порівнянні з тими перевагами, які хоче отримати особа, погодившись із його положеннями. В такому випадку особі слід окремо надати коротко та в доступному вигляді інформацію, визначену статтею 12 Закону.

Також не може вважатися доступною інформація, яка не надається особі перед наданням згоди безпосередньо, а натомість надається посилання на джерело, де міститься всі необхідні відомості. В якості прикладу можна навести поширену ситуацію, наприклад, із

отриманням кредиту, коли особа заповнює анкету та подає заяву, у якій, серед іншого, погоджується з умовами та правилами надання банківських послуг, що зазвичай розміщені на сайті банківської установи. У вказаних умовах дійсно міститься інформація щодо обробки персональних даних клієнта. Формально все вірно – особа має можливість ознайомитися з умовами до підписання заяви та анкети. Однак, на момент фактичного укладення договору така інформація відсутня в доступному вигляді, що призводить до того, що угода підписується без розуміння того, як оброблятимуться персональні дані, необхідні для її виконання.

Відтак, інформація щодо порядку обробки персональних даних повинна надаватися у вигляді, доступному для розуміння особою, яка не є спеціалістом у сфері законодавства про захист персональних даних.

Зазвичай володілець повинен отримати від суб'єкта персональних даних згоду на обробку його персональних даних у письмовому вигляді. Допускається будь-яка інша **форма** надання згоди (див. приклад, наведений нижче), однак володілець повинен мати змогу підтвердити наявність згоди впродовж всього часу здійснення обробки персональних даних. Вказане тлумачення підтверджується комплексним аналізом положень статті 2, 6 та 11 Закону. Інше розуміння є недопустимим, оскільки передбачатиме існування ситуацій, коли персональні дані оброблятимуться начебто на підставі згоди, яка нічим не підтверджується. Така обробка немає законних підстав, а відтак є незаконною.

ПРИКЛАД.

Благодійна організація, яка займається закупкою медичного обладнання та медикаментів для осіб хворих на діабет, звертається до департаменту охорони здоров'я з пропозицією розіслати серед лікарів-ендокринологів оголошення щодо проведення акції. Відповідно до її умов особи, які страждають на діабет, можуть зателефонувати за вказаним в оголошенні номером та зареєструватися (надати ім'я, прізвище, по батькові, телефон та домашню адресу) для участі в акції, за результатами якої вони безоплатно отримують ті чи інші необхідні їм медикаменти/обладнання. Після цього осіб повідомляють, коли та де можна отримати подарунки. При собі необхідно мати документи, які посвідчують особу та підтверджують наявність діабету.

Особи, які зареєструються, автоматично вважаються такими, що надали згоду на обробку персональних даних.

Укладення та виконання правочину

Укладення та виконання правочину як підстава для обробки персональних даних фактично також базується на основі згоди особи. Це підтверджується тим, що як і згода в її класичному розумінні (див. вище), правочин згідно з цивільним законодавством повинен відповідати низці вимог, які викладені в статті 203 Цивільного Кодексу України, відповідно до частини 3 якої «волевиявлення учасника правочину має бути **вільним** і **відповідати його внутрішній волі**».

Так, вільність волевиявлення фактично відповідає принципу добровільності, про який мова йшла вище, і передбачає право особи вирішувати вчиняти правочин чи ні. Відповідність внутрішній волі, хоч і не в повній мірі, але все ж охоплює принцип поінформованості, оскільки передбачає, що учасник правочину перед здійсненням волевиявлення повною мірою усвідомлює його правові наслідки.

Укладення правочину як підстава обробки персональних даних, необхідних для виконання правочину, також передбачає, що перед вчиненням правочину суб'єкту надаватиметься передбачена статтею 12 інформація у такому ж вигляді, як і у випадку надання окремої згоди (див. вище).

Різниця між правочином та згодою, як окремою підставою для обробки персональних даних лише в тому, що сам по собі договір (незалежно від змісту його положень) є підставою для обробки даних особи, незалежно від надання чи ненадання окремої згоди.

Закон

Обробка персональних даних на підставі закону передбачає наявність однієї з чотирьох підстав, визначених п.п. 2, 4, 5 та 6 ч.1 ст. 11 Закону:

- **дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;**

Як зазначалося вище, це положення сформульовано дещо нечітко. Так, аналіз даного положення створює враження, що для здійснення кожної обробки персональних даних щоразу необхідно передбачати відповідне право законом.

NOTA BENE!

Вказане трактування є неправильним і на практиці призвело до того, що велика кількість державних органів, що потребують обробки персональних даних для реалізації своїх повноважень, почали вимагати у суб'єктів згоду на обробку їх персональних даних, оскільки не було прямої норми закону, яка би була підставою для збору інформації.

Проте, аналогічне положення Директиви (див. вище) 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 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 нижче).

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. «б» ч. 2 ст. 12 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» при здійсненні заходів боротьби з організованою злочинністю спеціальним підрозділам по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України надаються повноваження: (...) на письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю одержувати від банків, а також кредитних, митних, фінансових та інших установ, підприємств, організацій (незалежно

від форм власності) інформацію і документи про операції, рахунки, вклади, внутрішні та зовнішні економічні угоди фізичних і юридичних осіб.

Таке положення дає право відповідним органам при здійсненні заходів боротьби з організованою злочинністю збирати інформацію, яка, серед іншого, містить персональні дані. Однак, його одного недостатньо для її збору, оскільки така інформація відповідно до п. 2 ч. 1 ст. 11 Закону повинна бути необхідною для здійснення офіційних повноважень володільця.

Відтак збір (та подальша обробка) персональних даних буде законним, якщо здійснюється в межах компетенції (тобто для боротьби з організованою злочинністю) та є необхідним для здійснення таких повноважень (є інформація щодо вчинення того чи іншого злочину, відкрите кримінальне провадження/оперативно-розшукова справа).

При цьому слід наголосити, що вказана підстава застосовується в основному до обробки персональних даних державними органами. Це підтверджується зокрема тим, що поняття **«повноваження»**, про яке йде мова у п. 2 ч. 1 ст. 11 Закону, практично не застосовується щодо юридичних осіб, окрім випадків, пов'язаних із представництвом юридичної особи (ст.ст. 240, 241, 243, 248 Цивільного кодексу України). Натомість вказане поняття зазвичай використовується, коли мова йде про державні органи, їх права та обов'язки (ст.ст. 19, 72, 77, 78, 81, 85, 89, 90, 105, 108, 110, 112, 115, 134, 144, 150 Конституції).

Слід наголосити, 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.

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.

У справі «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 в рамках розгляду справи про вчинення адміністративного правопорушення (п.п. 119–122 рішення).

ПРИКЛАД 2.

У справі «P.G. and J.H. v. The United Kingdom» під час перебування у відділі поліції заявників було записано під час розмови зі співробітниками поліції. Зразок їх голосу було збережено для проведення експертизи (в ході якої він порівнювався з іншими зразками, які нібито також належали заявникам). Заявники стверджували, що запис без їх відома голосу (навіть під час розмови з іншими особами – офіцерами поліції) з метою подальшого аналізу та використання становив порушення їх прав, гарантованих статтею 8 Конвенції. У зв'язку з цим Суд зазначив, що в законодавстві Великобританії не було норм, що регламентували би процес збору зразків голосу в приміщенні управління поліції. Відтак Суд констатував порушення прав заявників, гарантованих статтею 8 Конвенції (див. рішення у справі «P.G. and J.H. v. The United Kingdom», п.п. 61–63).

ПРИКЛАД 3.

Рішення ЄСПЛ у справі «Авілкіна проти Росії».

Фабула: В ході проведення перевірки діяльності релігійної організації свідків Єгови за скаргою, направленою ГО «Комітет спасіння молоді» (на думку ГО свідки Єгови заставляли своїх парафіян 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.

Рішення Суду: було втручання в права особи, гарантовані статтею 8 Конвенції.

Законність: є законні підстави для отримання інформації, але відповідні положення закону надто загальні. У зв'язку з цим Суд наголосив, що в такому випадку слід мати детальні норми щодо порядку та сфери

застосування вказаних положень закону, а також заходів захисту щодо порядку надання такої інформації, оскільки саме так забезпечуються достатні гарантії проти свавільності та зловживання. Однак, на думку Суду це питання тісно пов'язане з питанням необхідності.

Наявність легітимної мети: боротьба зі злочинністю.

Необхідність та пропорційність втручання (чи були мотиви на користь такого втручання співмірними, відповідними та достатніми переслідуваній меті – боротьба зі злочинністю):

- 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 примусу з боку братів по релігії з метою відмови від лікування;
- прокуратура не спробувала отримати згоду пацієнтів;
- не було порядку реалізації повноважень прокуратури на отримання документів;
- суди переглянули скаргу заявників, однак не задовольнили її (і що головне не встановили справедливого балансу інтересів, не надали обґрунтування передачі інформації), тим самим підтвердивши необмежені повноваження прокуратури.

Отже, відповідних та достатніх мотивів не було.

- **захист життєво важливих інтересів суб'єкта персональних даних;**

Аналогічна підстава обробки персональних даних передбачена п. «с» ч. 2 ст. 8 Директиви. За загальним правилом ця підстава передбачає, що на момент, коли виникла потреба захисту життєво важливих інтересів суб'єкта персональних даних, яка потребує, серед іншого, здійснення обробки його персональних даних, отримати згоду неможливо. На практиці причини можуть бути різними – перебування особи без свідомості, відсутність інформації щодо місця перебування особи, нездатність особи усвідомлювати наслідки вчинення своїх дій.

ПРИКЛАД.

Закон України «Основи законодавства України про охорону здоров'я»

Стаття 3. Поняття і терміни, що вживаються в законодавстві про охорону здоров'я

У цих Основах та інших актах законодавства про охорону здоров'я основні поняття мають таке значення: (...)

невідкладний стан людини – раптове погіршення фізичного або психічного здоров'я, **яке становить пряму та невідворотну загрозу життю та здоров'ю людини** або оточуючих її людей і виникає внаслідок хвороби, травми, отруєння або інших внутрішніх чи зовнішніх причин; (…)

Стаття 37. Надання медичної допомоги в невідкладних та екстремальних ситуаціях

Медичні працівники зобов'язані невідкладно надавати необхідну медичну допомогу у разі виникнення невідкладного стану людини.

Стаття 43. Згода на медичне втручання

Згода інформованого відповідно до статті 39 цих Основ пацієнта необхідна для застосування методів діагностики, профілактики та лікування. (…)

Згода пацієнта чи його законного представника на медичне втручання не потрібна лише **у разі наявності ознак прямої загрози життю пацієнта** за умови неможливості отримання з об'єктивних причин згоди на таке втручання від самого пацієнта чи його законних представників.

Вказані положення Закону України «Основи законодавства України про охорону здоров'я» передбачають, що у разі виникнення невідкладного стану людини надання їй медичної допомоги не потребує отримання її згоди. Будь-яке надання медичної допомоги тягне за собою необхідність обробки інформації про стан здоров'я. Невідкладний стан людини передбачає пряму та невідворотну загрозу її життю та здоров'ю. Відтак, обробка персональних даних, необхідних для надання медичної допомоги у невідкладних ситуаціях, здійснюється саме на підставі п. 4 ч. 1 ст. 11 Закону без згоди такої особи.

При цьому слід зважати на те, що відповідно до ч. 7 ст. 6 Закону, якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до того часу, коли отримання згоди стане можливим.

– **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 на перший погляд дещо перетинається із підставою, передбаченою п. 2 ч. 1 ст. 11 Закону, де мова йде про об-

робку у зв'язку з необхідністю виконання повноважень (прав та **обов'язків**). Однак, як вже зазначалося вище, підстава, передбачена п. 2 ч. 1 ст. 11 Закону, стосується в основному діяльності державних органів. Необхідність виконання обов'язків стосується ж *інших* володільців.

Це обумовлюється природою вказаних володільців (державних органів та *інших* володільців). Так, державні органи діють «лише на підставі, в межах повноважень та у спосіб, що передбачені конституцією та законами України». Відтак вони можуть обробляти лише ті дані, що обумовлюються їх повноваженнями, які є чітко визначеними законами.

Коли мова йде про володільців, чия діяльність носить приватноправовий (а тому більш диспозитивний) характер, то тут ситуація дещо інша. Очевидно, що обов'язки таких суб'єктів чітко визначені законодавством, а, отже, можна оцінити і об'єм персональних даних, необхідний для їх обробки.

Щодо прав таких суб'єктів слід зазначити, що їх коло є набагато ширшим. Більше того, *інші* володільці у своїх діях можуть керуватися не лише правами, а й законними інтересами, які якраз і є втіленням принципу «дозволено все, що не заборонено законом». Відтак інколи необхідність обробки персональних даних *іншими* володільцями обумовлюється наявністю у них законного інтересу.

Очевидно необхідність виконання обов'язку, передбаченого законом, виділено окремо, і саме з цих причин воно застосовується в основному до роботи володільців, що не є державними органами.

ПРИКЛАД 1.

Комунальне підприємство займається наданням житлово-комунальних послуг (наприклад, послуги з централізованого опалення, постачання холодної і гарячої води та водовідведення). Надання вказаних послуг та ведення їх обліку є обов'язком вказаного підприємства відповідно до статті 21 Закону України «Про житлово-комунальні послуги» та Правил надання послуг з централізованого опалення, постачання холодної і гарячої води та водовідведення, затверджених Постановою Кабінету Міністрів України від 21 липня 2005 року № 630 та очевидно потребує обробки низки даних суб'єктів (у даному випадку споживачів). Відтак обробка таких даних буде здійснюватися на законних підставах, оскільки обумовлюється обов'язками такого підприємства.

ПРИКЛАД 2.

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.

– **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**;

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.

Разом з тим, слід зазначити, вказане положення сформульовано не зовсім вірно, оскільки національне законодавство, по-перше, розділяє права та інтереси[9] і, по-друге, вказане положення дозволяє обробку з метою **захисту** законних інтересів, а відтак опускає їх **реалізацію**. Виходить, що Закон не передбачає можливості здійснювати обробку персональних даних приватно-правовими володільцями з метою реалізації прав та інтересів, а також з метою захисту прав. Якщо звернутися до положень Директиви, з якої вказане положення безперечно було взято, то побачимо, що його відповідник сформульований набагато зрозуміліше.

Так, Директивою дозволено обробляти персональні дані у випадку, *«якщо обробка необхідна для **цілей легітимних інтересів** володільця, третьої сторони чи сторін, кому передаються персональ-*

[9] Див. п. 3.6 Рішення Конституційного Суду України від 1 грудня 2004 року № 18-рп/2004 у справі за конституційним поданням 50 народних депутатів України щодо офіційного тлумачення окремих положень частини першої статті 4 Цивільного процесуального кодексу України (справа про охоронюваний законом інтерес).

ні дані, окрім випадків, коли такі інтереси перевищуються інтересами фундаментальних прав та свобод суб'єктів персональних даних, які потребують захисту за статтею 1 (1)».

Таким чином, у даному положенні мова йде власне про реалізацію та захист законних інтересів. Крім цього, поняття легітимного інтересу в контексті директиви є дещо ширшим і, на нашу думку, більше відповідає законним правам та інтересам, ніж формулювання, яке міститься у національному законодавстві[10].

Разом з тим вказане положення Закону слід розглядати в світлі положень Конвенції, а також відповідних Рекомендацій Комітету Міністрів Ради Європи, у яких мова йде про обробку персональних даних в цілях легітимного інтересу. Виходячи з цього, допустимою є обробка персональних даних з метою реалізації та захисту законних прав та інтересів.

Друга частина вказаного положення Закону «крім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес» наголошує на тому, що такі інтереси (права) обмежуються правами суб'єктів на захист їх персональних даних. Разом з тим обмеження щодо обробки персональних даних на підставі вказаного положення (легітимного інтересу), коли потреби захисту персональних даних переважають такий інтерес, є достатнім та не потребує додаткової умови про те, що суб'єкт персональних даних повинен вимагати припинити обробку його персональних даних. Це підтверджується Директивою («окрім випадків, коли такі інтереси перевищуються інтересами фундаментальних прав та свобод суб'єктів персональних даних, які потребують захисту за статтею 1 (1)» – тобто лише одна умова) та практикою Європейського суду з прав людини, згідно з якою втручання в право особи на повагу до приватності (а обробка персональних даних і є таким втручанням) є можливим лише за умови, коли суспільні інтереси переважують інтереси окремої особи (див. вказані вище рішення Європейського суду у справах «L.H. v. Latvia» та «S. and Marper v. The United Kingdom») і держава несе відповідальність за впровадження вказаного принципу (рішення у справі «I. v. Finland»).

Інші положення Закону, а саме статті 6, а також передбачають, що обробка персональних даних повинна бути пропорційною меті.

[10] Див. п. 3.5–3.6 вказаного Рішення.

3.4. 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 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.

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. 25 Кодексу законів про працю України (КЗПУ), відповідно до якої «при укладенні трудового договору гро-

мадянин 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».

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.

6) необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю.

Таким чином, допускається обробка медичної інформації для цілей 1) охорони здоров'я; 2) встановлення медичного діагнозу; 3) забезпечення піклування; 4) забезпечення лікування; 5) надання медичних послуг.

Відповідно до ст. 3 Закону України «Про основи законодавства України про охорону здоров'я», охорона здоров'я – це система заходів, які здійснюються органами державної влади та органами місцевого самоврядування, їх посадовими особами, закладами охорони здоров'я, медичними та фармацевтичними працівниками і громадянами з метою збереження та відновлення фізіологічних і психологічних функцій, оптимальної працездатності та соціальної активності людини при максимальній біологічно можливій індивідуальній тривалості її життя; медична допомога – діяльність професійно підготовлених медичних працівників, спрямована на профілактику, діагностику, лікування та реабілітацію у зв'язку з хворобами, травмами, отруєннями і патологічними станами, а також у зв'язку з вагітністю та пологами. Відтак поняття встановлення медичного діагнозу та лікування охоплюються поняттям «охорона здоров'я».

Відповідно до ст. 59 Цивільного кодексу, **піклування** встановлюється над неповнолітніми особами, які є сиротами або позбавлені батьківського піклування, та фізичними особами, цивільна дієздатність яких обмежена. Відповідно до ст. 36 Цивільного Кодексу України («Обмеження цивільної дієздатності фізичної особи»), суд може обмежити цивільну дієздатність фізичної особи, якщо вона страждає на психічний розлад, який істотно впливає на її здатність усві-

домлювати значення своїх дій та (або) керувати ними. Суд може обмежити цивільну дієздатність фізичної особи, якщо вона зловживає спиртними напоями, наркотичними засобами, токсичними речовинами тощо і тим ставить себе чи свою сім'ю, а також інших осіб, яких вона за законом зобов'язана утримувати, у скрутне матеріальне становище.

Щодо поняття **медичних послуг** слід зазначити, що його визначення відсутнє в національному законодавстві[11], однак виходячи з термінології ВООЗ та Рішення Конституційного Суду України у справі про безоплатну медичну допомогу[12] видається, що поняття «медичні послуги» є ширшим за поняття «медичної допомоги». Так, КСУ у вказаному рішенні зазначив, що «не забороняє вказане положення (авт. – частина 3 статті 49 Конституції) і можливості надання громадянам медичних послуг, які виходять за межі медичної допомоги (за термінологією Всесвітньої організації охорони здоров'я – «медичних послуг другорядного значення», «парамедичних послуг»), у зазначених закладах за окрему плату. На це вже зверталась увага у Рішенні Конституційного Суду України від 25 листопада 1998 року № 15-рп/98». Більше того, з огляду на зміст, який вкладається Конституційним судом у поняття «медичні послуги», воно за певних умов виходить за межі поняття «охорона здоров'я»[13] (наприклад, коли мова йде про медичний огляд осіб для отримання посвідчення водія транспортних засобів, дозволу на право отримання та носіння зброї громадянами тощо).

Таким чином, усі вказані в п. 6 ч. 2 ст. 7 Закону легітимні цілі обробки, за винятком піклування та частково медичних послуг, охоплюються поняттям охорони здоров'я, що очевидно є найбільш загальним і включає встановлення медичного діагнозу, лікування та

[11] Абзац 1 пункту 3 Рішення Конституційного Суду України у справі за Конституційним поданням 53 народних депутатів України щодо офіційного тлумачення положення частини третьої статті 49 Конституції України «у державних і комунальних закладах охорони здоров'я медична допомога надається безоплатно» (**справа про безоплатну медичну допомогу**).

[12] Абзац 9 пункту 4 вказаного Рішення.

[13] Абзац 7 пункту 2 Рішення Конституційного Суду України у справі за Конституційним поданням 66 народних депутатів України щодо відповідності Конституції України (конституційності) Постанови Кабінету Міністрів України «Про затвердження переліку платних послуг, які надаються в державних закладах охорони здоров'я та вищих медичних закладах освіти» (**справа про платні медичні послуги**).

надання медичних послуг, які є частиною медичної допомоги. При цьому з огляду на виділення в окрему категорії піклування, що є наслідком обмеження дієздатності особи, незрозуміло, чому не було виділено в якості окремої цілі здійснення опіки, яка є наслідком визнання особи повністю недієздатною (внаслідок хронічного, стійкого психічного розладу не здатна усвідомлювати значення своїх дій та (або) керувати ними). Вирішення вказаних питань потребує внесення змін до Закону.

При цьому, обробка у вказаних цілях можлива лише, якщо здійснюється «медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю».

Відповідно до ст. 40 Закону України «Про основи законодавства про охорону здоров'я» («Лікарська таємниця»), медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків.

Таким чином, лише визначені працівники закладу охорони здоров'я мають право обробляти чутливі дані в цілях, визначених п. 6 ч. 2 ст. 7 Закону. Такий стан справ суперечить реаліям, оскільки обробка чутливих даних у вказаних цілях в дійсності здійснюється набагато ширшим колом суб'єктів (наприклад, з метою призначення тих чи інших видів соціальної допомоги, видачі дозволу на отримання та носіння зброї, отримання водійського посвідчення тощо)., якій в ході виконання професійних або службових обов'язків стала відома медична інформація, що розглядається як така, на яку поширюється законодавство про лікарську таємницю у світлі.

Формулювання цього положення не відповідає в цій частині вимогам частини 1 та 3 статті 8 Директиви, згідно з якою (1. Державичлени 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 правила-

ми, прийнятими компетентними національними органами, поширюється зобов'язання щодо збереження професійної таємниці, **чи іншою особою, на яку поширюються еквівалентні зобов'язання щодо конфіденційності**) та частинам 2–3 п. 3.2 Рекомендації Комітету Міністрів Ради Європи № R (97) 5 щодо захисту медичної інформації («В принципі медичні дані повинні збиратися та оброблятися лише спеціалістами-медиками ...»).

Відтак видається доцільним прибрати з п. 6 ч. 2 ст. 7 Закону поняття «заклад охорони здоров'я». Тоді, право обробляти чутливі дані належатиме медичним працівникам та іншим особам, на яких поширюється законодавство про лікарську таємницю. Виходячи з визначення лікарської таємниці, сюди належатимуть усі особи, яким у зв'язку з виконанням професійних чи службових обов'язків стали відомі ті чи інші чутливі дані.

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».

ПРИКЛАД.

Справа «L.H. v. Latvia».

У 1997 році у зв'язку з розривом матки заявниці, яка була на той момент вагітна, довелося терміново робити кесарів розтин та народжувати. В ході операції хірург без згоди на те заявниці провів їй перев'язку маткової труби, а відтак і стерилізацію. З огляду на те, що позасудового вирішення досягти не вдалося заявниця звернулася до суду з позовом про відшкодування шкоди за незаконну стерилізацію.

У 2004 році лікарня звернулася до Інспекції по якості надання медичної допомоги з проханням надати висновок щодо якості наданих заявниці медичних послуг.

Інспекція зібрала інформацію з 3-ох медичних установ щодо надання заявниці медичної допомоги з 1996 по 2003 роки та дійшла висновку про відсутність порушення прав заявниці.

В 2006 році за результатами розгляду позову заявниці суд присудив їй компенсацію за незаконну стерилізацію.

Заявниця оскаржила до суду факт збору чутливої інформації щодо неї Інспекцією, однак судами усіх інстанцій було відмовлено в задоволенні її позову з посиланням на Закон «Про захист персональних даних» та законодавство про охорону здоров'я.

Законодавство Латвії.

Закон про медичну допомогу: Інспекція здійснює контроль за якістю медичної допомоги.

Статут Інспекції: Інспекція має право розглядати скарги, проводити планові та позапланові перевірки за зверненнями, готувати висновки, звіти, збирати необхідну інформацію, давати рекомендації, накладати стягнення.

Стаття 11 Закону про захист персональних даних: обробка медичних даних можлива, якщо необхідна «в цілях лікування або організації надання медичних послуг».

Висновок ЄСПЛ. Щодо законності збору інформації про стан здоров'я заявниці Інспекцією, Інспекція мала право на збір інформації за зверненням установи (не лише за скаргами, як то наголошував заявник).

Досліджуючи питання необхідності збору інформації щодо заявниці ЄСПЛ зазначив про таке: збір інформації розпочався через сім років після надання медичних послуг, відтак сумнівно, що він здійснювався «в цілях лікування або організації надання медичних послуг».

Заявника не повідомляли, що на прикладі його справи здійснюється оцінка надання допомоги (так стверджував Уряд, натомість заявник говорив, що єдина мета – це надання доказів у справі). Жодних рекомендацій лікарні не надавали за результатами перевірки. Звіт стосувався дій одного з лікарів і був наданий якраз під час судового провадження щодо лікарні.

Суди не проаналізували, які саме норми стали підставою для отримання інформації, з якою саме метою (в загальному – оцінка якості надання медичної допомоги), а відтак не оцінили пропорційності.

Інспекція не запитувала заявника про надання згоди на оцінку якості медичної допомоги у його справі, не повідомляла про збір інформації про нього. Таким чином, позицію заявниці не було взято до уваги.

Твердження Уряду про те, що дослідження проводилося з метою визначитися, чи слід притягувати хірурга до відповідальності, також не могло відповідати дійсності. Так, строки притягнення до відповідальності до того часу закінчилися і не Інспекції було вирішувати, чи слід притягувати хірурга до кримінальної відповідальності.

Закон не встановлював жодних меж щодо збору чутливої інформації. Інспекцією було зібрано інформацію за період тривалістю сім років (за рік до операції та 6 після) з 3-ох установ, щоб оцінити одне хірургічне втручання. Цьому не було надано жодного обґрунтування.

Відтак, втручання не було законним і не містило достатніх гарантій проти свавілля.

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. При цьому, 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.

На завершення слід зазначити, що перелік підстав для обробки чутливих категорій персональних даних, передбачений статтею 7 Закону, видається надто обмежувальним і не охоплює всіх випадків, які передбачатимуть необхідність обробки таких даних. Більше того, як зазначалося вище, навіть не всі випадки, що передбачено Директивою, включені до 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.

В Україні відповідно до Закону «Про загальнообов'язкове державне соціальне страхування» в редакції від 13.03.2015 р. одним із завдань Виконавчої дирекції Фонду соціального страхування з тимчасової втрати працездатності є здійснення перевірки обґрунтованості видачі та продовження листків непрацездатності застрахованим особам (пункт 6 частина перша статті 9). З метою реалізації вказаних завдань Виконавча дирекція Фонду наділена повноваженнями отримувати документи та інформацію, які є необхідними для виконання покладених на неї завдань (ст. 10 Закону).

Таким чином, для виконання покладених на Дирекцію завдань, вона повинна мати можливість обробляти медичну інформацію про особу. Однак, стаття 7 Закону не вказує прямо таку ситуацію серед тих, що допускають обробку чутливих даних, оскільки в даному випадку мова не йде про питання охорони здоров'я чи надання медичної допомоги. Вказана ситуація прямо не пов'язана з реалізацією прав та обов'язків володільця у сфері трудових правовідносин, оскільки мова йде про здійснення контрольних повноважень.

Однак, право збирати медичну інформацію чітко визначене законом. Метою такого збору є «здійснення перевірки обґрунтованості видачі та продовження листків непрацездатності застрахованим особам». Видача таких листків передбачає здійснення відповідних виплат застрахованій особі, які здійснюють за рахунок коштів державного бюджету, а, отже, збір медичної інформації переслідує одну з передбачених статтею 25 Закону легітимних цілей, а саме – забезпечення економічного добробуту. Крім цього, збір такої інформації, якщо він здійснюється виключно в тому об'ємі, що є необхідним для перевірки обґрунтованості видачі та продовження листків непрацездатності, буде пропорційним.

Відтак у вказаній вище ситуації збір Дирекцією медичної інформації буде законним навіть незважаючи на те, що не охоплюється прямо положеннями статті 7 Закону.

ТЕМА 4. ПРАВА СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ ТА ШЛЯХИ ЇХ РЕАЛІЗАЦІЇ (ДОСТУП ДО ІНФОРМАЦІЇ ПРО СЕБЕ; ДОСТУП ДО ІНФОРМАЦІЇ ПРО ТРЕТІХ ОСІБ; ПРАВО НА ЗМІНУ, МОДИФІКАЦІЮ, ВИДАЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ; ПРАВО ЗНАТИ ПРО ПОРЯДОК ОБРОБКИ, АДЕКВАТНИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ).

4.1. 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.

Зобов'язання володільця виділено окремо від прав суб'єкта персональних даних, закріплених у статті 8 Закону, зокрема права знати про обробку його персональних даних та зміст таких даних. Однак, воно є очевидно результатом подальшого розвитку принципу справедливості обробки та одним з невід'ємних аспектів права суб'єкта знати про обробку його персональних даних. Більше того, часто воно є запорукою дотримання вказаного права, 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). Відтак, вказане зобов'язання володільця слід розглядати разом із правом особи знати про обробку її персональних даних.

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 видається нелогічною. Важко уявити, щоб у процесі здійснення оперативно-розшукової діяльності чи проведення певних слідчих дій, 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 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[14]. Також є певні обмеження щодо повідомлення суб'єкта, коли інформація збирається в наукових, статистичних чи історичних цілях. Проект Регламенту містить більш детальні винятки[15].

Закон, а саме статтю 12, слід доповнити певними винятками з обов'язку повідомляти суб'єкта про збір інформації щодо нього. І хоча 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 ре-

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

[15] 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; повідомлення становитиме порушення прав та свобод інших осіб.

зультатом 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[16].

У зв'язку з цим постає ще одне запитання, а саме щодо форми повідомлення. Закон такої форми не встановлює. В ідеалі рекомендується під розписку повідомляти кожного суб'єкта особисто. Однак, зрозуміло, що за певних умов таке зобов'язання буде надмірним. Тому допускається вжиття інших способів повідомлення, зокрема шляхом направлення односторонніх повідомлень чи розміщення інформації на веб-сайтах. Однак такі способи можливі лише, коли неможливо забезпечити направлення індивідуального повідомлення.

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 частиною першою 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 контр-

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

розвідувальної 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 об-

робки (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 (тим більше, що порушення вказаного положення не тягне за собою накладення жодних фінансових стягнень).

4.2. 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**, тобто по суті 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 моментом є доступ до інформації про джерела отримання персональних даних. Надання володільцем такої інформації пов'язане з запорукою дотримання принципу законності обробки. Так, лише надавши відомості про джерела отримання персональних даних, володілець зможе підтвердити законність їх обробки. З цією метою володілець повинен зберігати документи, щоб у разі необхідності мати можливість підтвердити надану суб'єкту інформацію (наприклад, підписану заявником згоду на обробку персональних даних чи договір про купівлю бази даних).

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**», особливо друга частина цього положення. Часто вказане положення розуміється як таке, що стосується лише майбутніх можливих операцій із персональними даними. Насправді практика європейських держав, які власне і запровадили вказане положення, 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 (авт. – персональні дані суб'єкта)». У справі «Мер і члени міської ради Роттердаму проти М.Е.Е. Ріджкебура»[17] Суд Європейського Союзу фактично надав тлумачення вказаного положення Директиви. Зокрема, 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 отриман-

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

ня 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 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 вказаних положень 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 (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 зверта-

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

ється із письмовим запитом щодо отримання, наприклад, 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.

Звісно 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 містити положення, які з урахуванням характеру даних та особливостей певної сфери обробки, передбачатимуть 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.

Разом із тим практика застосування вказаного положення Уповноваженим забезпечує більш дієвий захист прав суб'єкта персональних даних.

ПРИКЛАД.

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 Київського міського пологового будинку №1 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.

Відтак, 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.

4.3. 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; 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 інформації про суб'єкта матиме вагомі юридичні наслідки, володілець має право вимагати від суб'єкта підтвердження того, що персональні дані дійсно потрібно змінити. При цьому на заявника не повинен покладатися надмірний тягар доведення того, що персональні дані підлягають зміні.

У цьому зв'язку слід зазначити, що у статті 12 (с) Директиви, а відтак у всіх державах членах Європейського Союзу, передбачене також право суб'єкта на повідомлення третіх сторін, кому бути розкриті його дані, про будь-які зміни, видалення чи блокування персональних даних суб'єкта, крім випадків, коли це неможливо чи ви-

[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.

магає непропорційних зусиль. **Аналогічне зобов'язання повинне бути запроваджене і в національному законодавстві**. До того часу добросовісним володільцям рекомендується, незважаючи на відсутність законодавчого регулювання цього питання, дотримуватися вказаного правила.

ПРИКЛАД.

До Уповноваженого надійшла скарга, у якій заявниця стверджувала про те, що Банк, з яким у неї раніше були договірні відносини, поширює недостовірну інформацію щодо наявності у неї заборгованості колекторським компаніям та бюро кредитних історій.

З матеріалів, отриманих в ході провадження, встановлено, що у серпні 2012 року між Банком та заявницею був укладений споживчий кредитний договір. Датою остаточної оплати заборгованості відповідно до графіка платежів як невід'ємної частини кредитного договору було визначено лютий 2014 року. Проте, відповідно до умов кредитного договору, станом на листопад 2012 року заявниця виконала свої зобов'язання по сплаті кредитної заборгованості шляхом її дострокового погашення.

Однак, у березні 2014 року від Банку заявниця отримала повідомлення про передачу справи до колекторської компанії у зв'язку з порушенням умов кредитного договору.

З метою захисту своїх прав заявниця звернулась до суду із позовом до Банку про захист прав споживача та визнання зобов'язань по кредитному договору виконаними. Рішенням суду першої інстанції, яке своєю чергою залишено без змін ухвалою апеляційного суду, визнано зобов'язання заявниці по кредитному договору між нею та Банком припиненими. З наведеного випливало, що заявниця виконала свої зобов'язання по сплаті кредитної заборгованості шляхом її дострокового погашення, а відтак будь-яка інформація, яка зберігалася та була поширена Банком щодо наявності в заявниці простроченої заборгованості за кредитом (зокрема, колекторській компанії, бюро кредитних історій), була недостовірною. Наявні в матеріалах провадження документи свідчили про те, що Банком дійсно було поширено вказаним суб'єктам інформацію щодо наявності у заявниці простроченої заборгованості за кредитом. Вимоги заявниці щодо виправлення неправдивої інформації щодо неї банком було проігноровано.

Відповідно до частини другої статті 6 Закону персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки. Відповідно до ст. 8 Закону суб'єкт персональних даних має право 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. Згідно зі статтею 20 Закону володільці та розпорядники зобов'язані вносити відповідні зміни на підставі **вмотивованої** вимоги.

У даній справі судами було встановлено, що заявниця здійснила дострокове погашення заборгованості по кредитному договору, тому її вимога щодо відповідної зміни її персональних даних була достатньо вмотивованою. Невиконання такої вимоги, на думку Уповноваженого, становило порушення вказаних прав заявниці, гарантованих Законом.

Також очевидно, що володілець, який поширив неправдиву інформацію щодо суб'єкта персональних даних, несе також відповідальність за її виправлення третіми особами. Інше розуміння призвело би до покладення на заявника надмірного тягаря. Крім того, згідно із Законом володілець повинен володіти інформацією щодо суб'єктів, яким передавалися персональні дані суб'єкта (див. вище). Тому повідомлення їх щодо необхідності внесення змін/видалення персональних даних суб'єкта не становитиме для нього надмірного тягаря.

Отже, з метою приведення в актуальний стан персональних даних заявниці Уповноваженим на підставі пункту 5 частини першої статті 23 Закону Банку направлено припис про невідкладне вжиття заходів щодо актуалізації персональних даних заявниці, як тих, що оброблялися Банком, так і тих, що передавалися Банком іншим організаціям та установам у період з моменту укладення споживчого кредитного договору до моменту отримання відповідного припису. Зокрема, на підставі частини другої статті 10 у відповідності до частини 2 статті 7 Закону України «Про організацію формування та обігу кредитних історій» подати до бюро кредитних історій достовірні відомості про грошове зобов'язання заявниці та вжити заходів направлених на видалення даних про її заборгованість, які були передані колекторській компанії.

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. Відтак, аналіз цих статей слід почати зі статті 15, яка містить дуже звужений перелік підстав для видалення персональних даних.

Відповідно до ст. 15 Закону персональні дані видаляються після закінчення строку, на який особа дала згоду. Однак, з урахуванням положень пункту 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 суб'єкт персональних даних відкликає згоду на оброб-**

ку персональних даних. Після закінчення вказаного строку чи відкликання згоди, якщо у володільця немає інших підстав для обробки даних, будь-яка подальша обробка буде незаконною. Відтак, це положення статті 15 повністю узгоджується зі статтею 8 Закону (п.п. 6 та 11 ч. 2 ст. 8).

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, або невизначений, або
- 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 певного 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 метою. Разом з тим, якщо інші підстави продовжують існувати, банк не зможе видалити персональні дані, необхідні для їх досягнення.

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

Щодо такої підстави для видалення, як «припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом», то вона є дово-

лі 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) українському законодавству та 2) Закону. При цьому друга вимога є набагато ширшою за своїм змістом.

Так, невідповідність законодавству передбачає, що або жодним нормативно-правовим актом не передбачено право обробляти персональні дані суб'єкта, або закон є надто загальним та нечітким і не визначає достатньою мірою порядок обробки персональних даних (див. вище розділ щодо принципу законності).

Разом із тим навіть, якщо іншими законами передбачено право обробляти персональні дані та визначено порядок такої обробки, вона повинна відповідати Закону України «Про захист персональних даних», зокрема викладеним у ньому принципам 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 поло-

женням Закону, то останньому слід розглянути можливість призупинення обробки та 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 розвести 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.

Крім цього, відповідно до частини другої 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, 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.

Крім цього, суб'єкт відповідно до вказаних положень Директиви, може заперечувати проти обробки його персональних даних із метою здійснення цільового маркетингу (який фактично і охоплюється пунктом 6 частини першої статті 11 Закону).

При цьому володільці повинні вжити заходів із метою доведення до відома суб'єктів факту наявності у них такого права (у випадку цільового маркетингу суб'єкту окремо повинна бути надана можливість заперечити до першої передачі його даних третій особі проти такої передачі).

Таким чином, якщо право на припинення обробки стосується даних, які обробляються незаконно, то 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 попереднього права та передбачає, що особа повинна бути попереджена/повідомлена про такий механізм автоматизованої обробки.

Це явище отримало назву профайлингу, який згідно з Регламентом є заходом, що має юридичні наслідки для особи або суттєво впливає на особу та базується повністю на автоматизованій обробці, метою якої є оцінити певні особисті сторони особи чи проаналізувати/передбачити, наприклад, працездатність особи, майновий стан, місцезнаходження, стан здоров'я, особисті вподобання, надійність чи поведінку.

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 (самостійно працівниками володільця чи 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 (в цьому і є суть права на захист від автоматизованого рішення, яке має для неї правові наслідки).

4.5. ІНШІ ПРАВА СУБЄКТА ПЕРСОНАЛЬНИХ ДАНИХ

Відповідно до частини другої статті 8 Закону суб'єкт персональних даних має право на 1) 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 на обробку своїх персональних даних до Уповноваженого або до суду та 3) застосовувати засоби правового захисту в разі порушення законодавства про за-

хист 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 документи з листування із володільцем). 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. Це є також особливо важливим з огляду на обмежені ресурси контролюючого органу та велику кількість потенційних володільців.

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**. Саме володілець повинен у разі направлення суб'єктом скарги мати можливість довести, що ним не було вчинено порушення, та надати відповідні докази. Відтак, він повинен бути сам зацікавлений у фіксації всіх дій, пов'язаних з обробкою персональних даних. 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 нестиме за нього відповідальність.

Звідси, а також з низки інших норм, про які мова йтиме в розділі щодо захисту персональних даних, логічно випливає зобов'язання володільця в розумних межах документувати процеси, пов'язані з обробкою персональних даних.

Отже, 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. Зокрема, мова може йти про наступне:

1. Суб'єкта автоматично інформують 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.

Таким чином, зрозуміло, що неправомірне приховування факту обробки суттєво зменшує можливості суб'єкта щодо реалізації решти його прав. Ненадання інформації у відповідь на його запит позбавляє суб'єкта можливості розібратися з тим, які дані обробляються, чи законно вони обробляються, чи відповідають вони дійсності тощо, а, відтак, вжити заходів щодо виправлення потенційних порушень.

ТЕМА 5. ОБМЕЖЕННЯ ДІЇ ПРАВ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ.

Відповідно до частини 1 статті 25 Закону, обмеження дії статей 6, 7 і 8 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. Стаття 6 закріплює основні принципи обробки персональних даних, про які мова йшла вище, стаття 7 – підстави обробки чутливих даних, а стаття 8 – права суб'єкта персональних даних.

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.

Вказані обмеження повністю відповідають тим, що передбачені чинною редакцією Конвенції. Однак, тут виникає доволі цікаве протиріччя: виходить, що обмеження до принципів законності, легітимної мети та необхідності повинні бути законними, необхідними та переслідувати легітимну мету. Така постановка питання частково нівелює сутність вказаного обмеження в частині, що стосується вказаних трьох принципів.

ПРИКЛАД.

В цілях національної безпеки окремим законом передбачено право низки державних органів збирати відомості щодо іноземців та осіб без громадянства. Склад таких відомостей однаковий для всіх іноземців та включає, серед іншого, відомості щодо перетину кордону, порушення режиму державного кордону та порядку перебування на території держави.

У зв'язку з початком збройного конфлікту із сусідньою державою до закону внесено зміни, відповідно до яких санкціоновано збір великої кількості інформації саме щодо осіб, які є громадянами вказаної держави. Вказані зміни регламентують порядок збору, зберігання, захисту, підстави поширення та доступу до такої інформації, строки її зберігання, умови видалення, а також механізми захисту прав відповідних суб'єктів.

Відтак, з одного боку **відбулося обмеження принципу необхідності**, оскільки щодо громадян однієї з держав збирається суттєво більше інформації, аніж щодо громадян інших держав. З другого боку **таке обмеження** передбачено законом, переслідує легітимну мету (національна безпека) і **є необхідними в її світлі** (посилена загроза з боку саме представників певної держави), що в свою чергу є запорукою дотримання відповідних принципів захисту персональних даних.

Вказане вище свідчить про те, що фактично не може бути жодних обмежень до принципів легітимної мети, необхідності та законності. Така позиція підтверджується і положеннями проекту модернізованої редакції Конвенції. Так, у вказаному документі статтю 5 Конвенції розбито на три частини:

1) обробка персональних даних повинна бути пропорційною щодо легітимної мети, яку вона переслідує, та відображати на всіх стадіях обробки справедливий баланс між усіма інтереса-

ми, яких вона торкається, приватними чи публічними та правами та свободами, що стоять на кону;

2) Кожна сторона передбачатиме, що обробка персональних даних може здійснюватися на підставі вільної, конкретної, поінформованої та однозначної згоди суб'єкта персональних даних чи на іншій легітимній підставі, передбаченій законом.
3) Третьою частиною статті передбачено дещо модифікований перелік принципів обробки, що передбачені чинною редакцією статті 5 Конвенції

При цьому стаття 9 модернізованої редакції Конвенції передбачає виключення лише до третьої частини. Відтак, жодних обмежень не дозволено застосовувати щодо принципів пропорційності, легітимної мети та наявності законних підстав обробки персональних даних.

Також слід зазначити, що як Директивою, так і Конвенцією передбачено набагато ширший перелік цілей, які використовуються для обмеження вищезазначених принципів обробки та прав суб'єкта.

Директива	**Конвенція**
Національна безпека; Оборона; Громадська безпека; Запобігання, розслідування, виявлення та переслідування кримінальних правопорушень чи порушень етики певних професій; Важливі фінансові та економічні інтереси держави, включаючи монетарні, бюджетні та податкові питання; Нагляд, інспекція чи регуляторна, які пов'язані, навіть випадково, з реалізацією офіційних повноважень у випадках, про які йде мова в п.п. c[20], d[21] та e[22]; Захист суб'єкта персональних даних чи прав та свобод інших.	Державна безпека; Громадська безпека; Монетарні інтереси держави; Боротьба зі злочинністю; Захист суб'єкта персональних даних чи прав та свобод інших. У проекті модернізованої версії Конвенції станом на березень 2015 року додатково вказано в якості цілей економічні та фінансові інтереси, запобігання злочинам, а серед прав та свобод інших особливо виділено право на свободу висловлення думки.

[20] громадська безпека

[21] запобігання, розслідування, виявлення та переслідування кримінальних правопорушень чи порушень етики певних професій

[22] важливі фінансові та економічні інтереси держави, включаючи монетарні, бюджетні та податкові питання

Звісно, що ті цілі, які передбачено в чинній редакції статті 25 Закону, є достатньо широкими, щоб поширити їх в ході застосування на практиці на всі випадки, що вказані у Директиві та Конвенції. Наприклад, вказані цілі, серед іншого, логічно включають боротьбу зі злочинністю у відповідній сфері – злочинами, що загрожують національній безпеці, економічному добробуту та правам інших людей[23]. Однак, для того, **щоб усунути будь-які сумніви у цій частині видається за доцільне внести відповідні зміни до статті 25 та розширити (а що важливіше деталізувати) перелік допустимих цілей обмеження основних принципів та прав суб'єкта персональних даних**. Це буде логічно і з тих міркувань, про які мова йшла вище, а саме, чим чіткішим є формулювання цілі, тим жорсткіше регламентовані можливі втручання в права особи на повагу до її приватності.

Разом із тим за умови дотримання положень статті 25 Закону можна обмежити застосовність принципу прозорості, відкритості, а також прав суб'єкта персональних даних. 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). Крім цього, батьки (усиновлювачі), опікун, піклувальник мають право на отримання інформації про стан здоров'я дитини або підопічного (частина 2 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 встанов-

[23] Принцип побудови Особливої частини Кримінального кодексу України, яка встановлює кримінальну відповідальність, зводиться до поділу всіх злочинів: на ті, які спрямовані проти основ національної безпеки, злочини у сфері господарської діяльності (економічні злочини), а також ті, які порушують те чи інше право людини.

лене 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).

Кожне таке обмеження має бути визначене законом, переслідувати легітимну мету та бути обґрунтованим із точки зору його необхідності.

ПОЗИЦІЯ УПОВНОВАЖЕНОГО

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.

Персональні дані щодо стану здоров'я Законом України «Про захист персональних даних» (далі – Закон), про які мова йшла в справі, 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) допускається обмеження дії положень статті 7 Закону. За обставин даної справи це означає, що «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**» 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 керівництво та управління загальнообов'язковим

державним соціальним страхуванням від нещасного випадку, у зв'язку з тимчасовою втратою працездатності та медичним страхуванням, провадить акумуляцію страхових внесків, контроль за використанням коштів, забезпечує фінансування виплат за цими видами загальнообов'язкового державного соціального страхування та здійснює інші функції згідно із затвердженим статутом.

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 ст. 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».

Нарешті, доцільно коротко зупинитися на розумінні «державної таємниці, як підстави для обмеження положень Закону. Це поняття міститься у статті 32 Конституції України і згідно із ним «не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. 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**». Так, віднесення інформації про особу до державної таємниці є також прикладом об-

меження принципу справедливості/прозорості обробки персональних даних, зокрема, як видно із вказаного вище положення Конституції, в частині, що стосується права особи на доступ до інформації про себе.

У цьому зв'язку слід зазначити, що 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. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю. Порядок доступу до таємної інформації регулюється цим Законом та спеціальними законами.

Згідно з частиною другою статті 6 Закону 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** та в порядку, визначеному законами (стаття 6 та 8 Закону України «Про доступ до публічної інформації»), **в цілях, передбачених пунктом 1 частини другої статті 6 вказаного Закону**. Вказані цілі загалом узгоджуються з тими, що передбачені статтею 25 Закону, однак ще раз підтверджують, що в цій частині статтю 25, як вже зазначалося вище, слід деталізувати. 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.

Вказане є ще одним прикладом застосування обмежень дії статей 6, 7 та 8 Закону.

ТЕМА 6. ПОРЯДОК ОРГАНІЗАЦІЇ ВОЛОДІЛЬЦЕМ ПРОЦЕСУ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

Захист персональних даних володільцем

6.1. ПОНЯТТЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

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

Перш за все, 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. При цьому слід враховувати вимоги законодавства у сфері захисту персональних даних та інформаційної безпеки. Вказана вимога стосується усіх володільців. 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.

3.3. Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

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.

(…)

3.12 Вимоги щодо обліку та збереження інформації про перегляд персональних даних не поширюються на володільців/розпорядників, які здійснюють обробку персональних даних в реєстрі, який є відкритим для населення в цілому.

3.13. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

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.

Володілець (підприємство, що займається роздрібною торгівлею) веде базу даних, в яку включаються такі категорії даних про 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 протягом останніх __ років.

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.

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 з вбудованою мікросхемою, 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 (див. у цьому зв'язку роз'яснення щодо використання біометричних замків вище у розділі про принципи захисту персональних даних). Залежно від важливості інформації, що зберігається в базі даних, приміщення можуть обладнуватися автоматичними електронними замками, сигналізацією, гратами на вікнах та дверях тощо. В якості додаткового заходу безпеки володільці можуть (з дотриманням певних гарантій) із метою контролю за виробничою дисципліною, дотриманням правил трудової етики здійснювати відеоспостереження за працівниками (про це мова йтиме в окремому розділі).

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 23 проекту 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 є доволі жорсткими та не враховують особливостей того чи іншого володільця (зокрема, його фінансових можливостей, масштабів обробки персональних даних, характеру даних). Натомість вони вибудовують систему хоч і потужного, але дорогого захисту.

6.2. Крім цього, як зазначалося вище, саме володілець повинен 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).

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

(...)

Вказане зобов'язання володільця є не лише результатом комплексного аналізу норм Закону. Його доцільність та обґрунтованість підтверджується чинними міжнародними документами та практикою Європейського суду з прав людини (див. Приклад 1 нижче), а також реальними потребами обробки та захисту персональних даних в Україні (див. Приклад 2 нижче).

ПРИКЛАД 1.

У справі «I. v. Finland», що розглядалася Європейським судом з прав людини, заявниця була особою, хворою на СНІД. Вона проходила лікування у тій же лікарні, де і працювала. Працівниками лікарні було розголошено інформацію про хворобу заявниці. Вона, своєю чергою, звернулася зі скаргою до адміністративного органу, а потім до суду. Їй було відмовлено в задоволенні скарг у зв'язку з тим, що відсутні докази того, що інформацію було незаконно переглянуто (так, вказаними органами було зазначено, що «якщо навіть були спроби отримати дані зі справи заявниці, цих осіб встановити неможливо, оскільки система обробки даних надає інформацію лише стосовно останніх п'яти запитів і лише стосовно відділення, з якого було здійснено запит, а не стосовно особи». При цьому навіть зазначена інформація була видалена після передачі справи заявниці в архів). 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 безпеки доступу та поширенням інформації про стан її здоров'я. Проте, перенесення такого тягаря доказування на заявницю свідчить про ігнорування відомих на той час недоліків у системі ведення документації в лікарні. Адже, 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 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.

У 2015 році до Уповноваженого звернулася заявниця зі скаргою про те, що співробітниками КЗОЗ «____ міська поліклініка № __» (далі – поліклініка) __.__.2015 їй було повідомлено про те, що її медична картка зникла з поліклініки. При цьому про причини та обставини зникнення медичної картки заявниці повідомлено не було. Заявниця пов'язує зникнення своєї медичної картки з тим, що у ній був зафіксований факт її звернення до дільничного терапевта __.__.2014 після того, як вона була піддана нена-

лежному поводженню з боку працівників _____ РВ ___ ГУ УМВС України в _____ області.

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 передавалася. Вказану інформацію слід було підтвердити відповідними документами.

У відповідь керівник поліклініки вказала, що медична картка заявниці ніколи не зберігалася в поліклініці. Більше того, за її словами дільничний лікар бачила медичну картку заявниці у неї вдома.

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, чий виклад фактів (заявниці чи керівника поліклініки) відповідає дійсності.

Так, в журналі видання та повернення амбулаторних карток міститься інформація щодо видачі та повернення медичних карток пацієнтів. Однак, в поліклініці відсутній загальний опис медичної документації, що є в її володінні. Відтак, не виключено, що якщо заявниця не зверталася за отриманням своєї медичної карти раніше, про її наявність не буде вказано в жодному офіційному документі поліклініки.

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 вказаних вище не-

законних дій, якщо він не володіє інформацією щодо того, які дані та у яких суб'єктів вони зберігаються. За таких обставин будь-яка операція (наприклад, втрата персональних даних) може бути списана на те, що володілець ніколи таких даних не обробляв.

– п. 3.11 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого від 8 січня 2014 року № 1/02–14:

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

Це положення, прийняте на виконання вказаних вище норм закону, деталізує їх та встановлює строки зберігання відомостей, що стосуються обробки персональних даних.

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.**

6.3. СТАТУС ОСІБ ТА СТРУКТУРНИХ ПІДРОЗДІЛІВ, ВІДПОВІДАЛЬНИХ ЗА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

За певних умов володільці зобов'язані призначити структурний підрозділ або відповідальну особа, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці.

Відповідно до ч. 2 ст. 24 Закону, в органах державної влади, органах місцевого самоврядування, а також у володільця чи розпоряд-

ника персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону (більш детально про функціонування системи повідомлення див. у відповідному розділі), створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці.

Щодо володільців та розпорядників, які здійснюють обробку, яка підлягає повідомленню, слід зазначити, що відповідно до ст. 9 Закону 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 із 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, визначаються Уповноваженим.

Види обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, визначено Порядком повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації, затвердженим наказом Уповноваженого від 08.01.2014 № 1/02–14 «Про затвердження документів у сфері захисту персональних даних» (далі – Порядок).

ПОРЯДОК.

1.2. Для цілей цього Порядку обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів – це будь-яка дія або сукупність дій, а саме збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем, яка здійснюється відносно персональних даних про:

- расове, етнічне та національне походження;
- політичні, релігійні або світоглядні переконання;
- членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;
- стан здоров'я;

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

(…)

2.1. Володілець персональних даних повідомляє Уповноваженого про здійснення ним будь-яких видів обробки персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, крім випадків, якщо:

2.1.1. здійснюється обробка, єдиною метою якої є ведення реєстру для надання інформації населенню, який відкритий для населення в цілому;

2.1.2. обробка здійснюється громадськими об'єднаннями, політичними партіями та/або організаціями, професійними спілками, об'єднаннями роботодавців, релігійними організаціями, громадськими організаціями світоглядної спрямованості за умови, що обробка стосується виключно персональних даних членів цих об'єднань та не передається без їх згоди;

2.1.3. обробка необхідна для реалізації прав та виконання обов'язків володільця персональних даних у сфері трудових правовідносин відповідно до закону.

Відтак, усі суб'єкти, які здійснюють обробку визначених п. 1.2 Порядку категорій персональних даних, за винятком тих, чия обробка охоплюється п. 2.1 Порядку, зобов'язані створити підрозділ/призначити особу, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці.

Компетенція та повноваження такої особи чи підрозділу в деталях визначаються володільцем у його внутрішніх документах, а загальні вимоги щодо їх статусу визначено Законом та Типовим порядком обробки персональних даних.

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.

ТИПОВИЙ ПОРЯДОК ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.17. Відповідальна особа/структурний підрозділ виконує такі завдання:

- інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;
- 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.

3.18. З метою виконання вказаних завдань відповідальна особа/структурний підрозділ:

- забезпечує реалізацію прав суб'єктів персональних даних;
- користується доступом до будь-яких даних, які обробляються володільцем/розпорядником та до всіх приміщень володільця/розпорядника, де здійснюється така обробка;
- у разі виявлення порушень законодавства про захист персональних даних та/або цього Порядку повідомляє про це керівника володільця/розпорядника з метою вжиття необхідних заходів;
- аналізує загрози безпеці персональних даних.

3.19. Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних.

3.20. Факти порушень процесу обробки та захисту персональних даних повинні бути документально зафіксовані відповідальною особою або структурним підрозділом, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

ПРАКТИКА ЗАСТОСУВАННЯ ВКАЗАНОГО ЗАКОНОДАВСТВА УПОВНОВАЖЕНИМ.

Працівниками Секретаріату Уповноваженого було проведено перевірку одного з районних управлінь ГУМВС (далі – РУ ГУМВС) на предмет законності обробки дактилоскопічних даних (див. більш детально про вказану перевірку вище). За результатами звірки за період з 01 січня до 20 листопада 2014 року було виявлено 508 осіб, стосовно яких відсутні підстави для їх дактилоскопіювання.

Додатково слід зазначити, що Закон України «Про міліцію» та Інструкція про порядок функціонування дактилоскопічного обліку експертної

служби МВС України, затверджена наказом МВС України від 11 вересня 2001 року, № 785 встановлюють низку вимог до обробки дактилоскопічних даних володільцем (у цьому випадку РУ ГУМВС), які узгоджуються з положеннями законодавства про захист персональних даних та забезпечують їх додержання в ході здійснення обробки дактилоскопічних даних і ведення дактилоскопічного обліку. Зокрема, вказані документи покладають на органи внутрішніх справ (далі – ОВС) як на володільців персональних даних (в частині обробки біометричних даних – відбитків пальців рук фізичних осіб) такі обов'язки:

- призначити у відповідних структурних підрозділах ОВС працівників відповідальних за організацію взяття на дактилоскопічний облік (п. 2.1.15. Інструкції), що узгоджується з положенням ч. 2 ст. 24 Закону. Такі особи зокрема зобов'язані вести облік дактилоскопійованих осіб (наприклад, у Журналах обліку дактилокарт);
- вести Журнали обліку дактилокарт за напрямками діяльності у відповідних структурних підрозділах ОВС, які здійснюють заходи із організації взяття на дактилоскопічний облік (п. 2.1.15 Інструкції). При цьому відповідно до п. 2.2.4 Інструкції дактилокарта на особу, серед іншого, має містити відомості про підстави дактилоскопіювання та посаду, прізвище і підпис працівника, який заповнив дактилокарту. Ці вимоги Інструкції відповідають п. 3.11 Типового порядку обробки.

За результатами перевірки було встановлено, що керівництвом РУ ГУМВС не було призначено працівників, відповідальних за організацію взяття на дактилоскопічний облік, журнали обліку дактилокарт не велися, а дактилокарти були заповнені не повністю (не вказувалися підстави дактилоскопіювання та особа, яка його здійснила).

Недотримання вказаних положень Закону призвело до таких наслідків:

- дактилокарти та журнал (де вказується, кого було дактилоскопійовано, хто із співробітників проводив дактилоскопіювання та його підстави) не велися належним чином, а відтак неможливо було встановити конкретних працівників, чиї дії призвели до незаконного дактилоскопіювання;
- РУ ГУМВС не володіло, а відтак, не змогло надати представникам Секретаріату Уповноваженого інформації щодо осіб, яких було дактилоскопійовано. Такі дії суттєво ускладнюють перевірку законності ведення дактилоскопічного обліку (див. вище) та фактично позбавляють суб'єктів персональних даних можливості отримати інформацію щодо того, чи обробляються та як обробляються їх персональні дані (відбитки пальців), а, отже, реалізувати свої права, гарантовані статтею 8 Закону.

Фактично питання щодо дактилоскопіювання осіб вирішувалося великою кількістю оперативних співробітників (кожен щодо своїх справ), які зацікавлені в проведенні дактилоскопіювання, оскільки воно в тій чи іншій мірі полегшує їх роботу (зокрема, якщо під час огляду місця події

виявлені пальців відбитки ймовірного порушника). При цьому відсутня особа, яка не займається конкретним розслідуванням і яка повинна була би проконтролювати ведення журналу (де вказується, кого було дактилоскопійовано, хто із співробітників проводив дактилоскопіювання та його підстави), а також заповнення дактилокарт.

У зв'язку з цим Уповноваженим було винесено припис щодо усунення вищезазначених недоліків.

Основне завдання такої особи налагодити належним чином порядок обробки персональних даних володільцем. Якщо володільцем було вжито всіх необхідних заходів захисту чи відповідальна особа донесла до відома керівництва інформацію про те, яких заходів слід було вжити (однак їх не було вжито), вона не нестиме відповідальності за порушення законодавства про захист персональних даних.

В залежності від операцій з обробки, що здійснюються володільцем, та характеру персональних даних володілець самостійно визначає компетенцію та повноваження такої особи/підрозділу. Зазвичай сюди можуть належати такі:

– **проводити оцінку ризиків від обробки персональних даних володільцем;**

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. В разі потреби такі висновки можуть бути викладені в окремому документі.

У цьому зв'язку варто зазначити, що згідно з проектом Регламенту в разі, якщо володільцем здійснюється обробка персональних даних, що може становити ризик для прав та свобод суб'єктів, він зобов'язаний проводити таку оцінку.

– **надавати з урахуванням проведеної оцінки консультацій володільцю щодо належної організації процесу обробки персональних даних (та документувати цю діяльність)**,

а саме 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, чіткого визначення повноважень осіб, що залучені до процесу обробки персональних даних та ін.. Загалом, коли мова йде про велику компанію, робота відповідальної особи в цій частині передбачатиме підготовку узгодженої з іншими підрозділами політики приватності компанії (та в разі потреби інших документів, що регламентують порядок обробки та захисту персональних даних). 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. В ідеалі такі документи не повинні прийматися без погодження такої особи;

- **в разі необхідності (зокрема, коли мова йде про невеликі компанії) до завдань відповідальної особи/підрозділу може бути віднесено зберігання документації щодо обробки персональних даних, розгляд запитів суб'єктів та третіх осіб щодо отримання доступу до персональних даних, прийняття рішення щодо надання доступу до персональних даних працівникам та інше;**
- **моніторинг процесів обробки персональних даних на предмет їх відповідності політиці приватності володільця;**

Так, відповідальна особа/підрозділ повинна здійснювати контроль за дотриманням працівниками володільця чи розпорядника політики приватності (наприклад, з метою моніторингу законності доступу до персональних даних переглядати журнал обліку операцій, пов'язаних з обробкою персональних даних), актуалізувати інформацію щодо потенційних ризиків (див. вище), переглядати в разі потреби організаційні та технічні заходи захисту персональних даних, порядок їх обробки з метою зокрема приведення їх у відповідність до нових ризиків (чи мінімізації втручання в права особи на приватність, внаслідок такої обробки), доводити результати роботи до відома керівництва, підтримувати в актуальному стані документи, що

регламентують порядок обробки персональних даних володільцем чи розпорядником.

– **вживати заходів у разі виявлення порушення законодавства про захист персональних даних;**

Якщо мова йде про порушення, що може мати серйозні наслідки для прав суб'єктів персональних даних, про це слід відразу доводити до відома керівництва та Уповноваженого, а також вживати/рекомендувати керівництву вжиття першочергових заходів, спрямованих на мінімізацію потенційних негативних наслідків. Окрім того, в разі наявності такої можливості про це порушення слід повідомляти самого суб'єкта/ів персональних даних.

– **ознайомлювати (організовувати процес ознайомлення) 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;**
– **взаємодія з Уповноваженим**, що може проявлятися у таких основних напрямках: 1) консультації з приводу доцільності та порядку обробки персональних даних володільцем, отримання з цього приводу роз'яснень Уповноваженого; 2) отримання висновку щодо розробленого кодексу поведінки відповідно до ст. 27 Закону (у випадку, коли мова йде по роботу державного органу, органу місцевого самоврядування – направляти Уповноваженому для погодження проекти нормативно-правових актів, що стосуються питань обробки персональних даних); 3) співпраця в ході розгляду Уповноваженим звернень громадян (надання необхідних документів та інформації); 4) співпраця 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); 5) забезпечення вчасного та повного виконання приписів Уповноваженого; 6) участь в освітніх, науково-практичних заходах, що проводяться Уповноваженим та працівниками Секретарі-

ату; 7) участь в разі необхідності в громадських радах, що діють при Уповноваженому; 8) надання вузькоспеціалізованих консультацій працівникам Секретаріату Уповноваженого;

З метою виконання такого широкого спектру завдань відповідальна особа/підрозділ повинні користуватися відповідними правами, які необхідні для належного виконання ними своїх посадових обов'язків, а саме право:

- безперешкодного доступу до приміщень, де здійснюється обробка персональних даних;
- 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;
- своєчасно отримувати повну інформацію щодо будь-яких операцій, пов'язаних з обробкою персональних даних, що здійснюються володільцем чи розпорядником;
- право безпосереднього звітування керівництву володільця чи розпорядника.

Для виконання вказаних вище завдань 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.

Посадова інструкція цієї особи/підрозділу, а також внутрішні установчі (статутні) чи розпорядчі документи володільця 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 рекоменда-

цій чи виконання певним чином їх обов'язків у сфері захисту персональних даних.

Слід зазначити, що, незважаючи на положення статті 24 Закону, усім володільцям, які здійснюють обробку великого об'єму персональних даних, рекомендується визначити відповідальну особу/підрозділ, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Порядок організації володільцем процесу обробки персональних даних

Відповідно до ст. 2 Закону, володілець – це фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом. Отже, мета обробки, склад даних та порядок їх обробки визначаються **або володільцем, або законом**.

У такому випадку, виходячи з принципу законності обробки персональних даних (див. вище) та положень Типового порядку обробки персональних даних, визначенню (володільцем чи законом) підлягають такі елементи:

1) мета та підстави обробки персональних даних;

Володілець (закон) повинен визначити та чітко сформулювати мету та підстави обробки персональних даних. Вказане питання є актуальним, оскільки воно дуже часто вирішується лише у зв'язку зі запитом суб'єкта чи в ході проведення перевірки уповноваженим.

2) категорії суб'єктів персональних даних;

Володілець (закон) повинен вказати, чиї персональні дані обробляються, (наприклад, клієнтів, учасників програми, акції, членів організації, працівників тощо).

3) склад персональних даних;

4) порядок обробки персональних даних, а саме спосіб збору, накопичення персональних даних;

В цій частині володілець (закон) повинен перш за все визначити, яким чином збираються персональні дані: безпосередньо у суб'єкта чи в інших володільців. Виходячи з цього, він повинен визначити, чи повідомляється суб'єкт про обробку його персональних даних. Якщо ні, то чому та які при цьому гарантії дотримання прав суб'єкта. Якщо не завжди повідомляється, то конкретно визначити випадки,

коли суб'єкт повідомляється, а коли ні, і які знову ж таки при цьому гарантії дотримання його прав. Якщо суб'єкт повідомляється, володілець повинен визначити, яка форма такого повідомлення.

– строк та умови зберігання персональних даних (крім випадів, коли вони уже визначені законом);

Володілець (закон) повинен визначити, які дані, щодо яких категорій суб'єктів та впродовж якого строку зберігаються. Це важливо, оскільки якщо строк визначено володільцем, а не законом, саме володілець повинен не лише назвати такий строк, а й бути готовим пояснити, чим обумовлюється саме такий строк зберігання.

– умови та процедуру зміни, видалення або знищення персональних даних;

Володілець (закон) повинен вказати перш за все порядок розгляду ним звернень суб'єктів персональних даних щодо припинення обробки/зміни їх персональних даних, порядок розгляду та виконання приписів Уповноваженого та рішень суду щодо зміни/видалення персональних даних, а також процедуру видалення персональних даних у разі закінчення строків їх зберігання чи з інших підстав.

– умови та процедуру передачі персональних даних та перелік третіх осіб, яким можуть передаватися персональні дані;

В цій частині володілець (закон), виходячи з положень закону та персональних даних, що ним обробляються, визначає суб'єктів, яким передаються (можуть передаватися персональні дані), підстави передачі в залежності від особи запитувача (запит-відповідь, договір), а, відтак, порядок розгляду запитів щодо доступу до персональних даних, вимоги щодо верифікації особи запитувача інформації, вимоги до договору про передачу персональних даних (у тому числі до іншої сторони договору). Також володілець визначає, чи здійснюється ним транскордонна передача даних та які підстави та умови такої передачі, вимоги, що ставляться до отримувача такої інформації та його зобов'язання щодо її збереження.

– порядок доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних;

Володілець (закон) зобов'язаний визначити, порядок надання суб'єктам доступу до інформації про порядок обробки їх персональних даних та змісту їх даних, що ним обробляються, зокрема спосіб верифікації особи, що запитує доступ.

Крім цього, володілець (закон) повинен визначити порядок розподілу доступу його працівників до персональних даних.

5) заходи забезпечення захисту персональних даних.

Володілець повинен визначити порядок обліку операцій, пов'язаних з обробкою персональних даних та доступом до них, а також надати детальний опис заходів захисту, що вживаються ним метою запобігання їх втраті, знищенню та незаконній обробці (про це мова йтиме нижче).

Слід також зазначити, що **усі вищезазначені елементи обробки персональних даних необхідно визначити до початку обробки**. За певних умов володілець до початку обробки персональних даних може також погодити її порядок з Уповноваженим. Так, відповідно до ст. 27 Закону «професійні, самоврядні та інші громадські об'єднання чи юридичні особи можуть розробляти кодекси поведінки з метою забезпечення ефективного захисту прав суб'єктів персональних даних, додержання законодавства про захист персональних даних з урахуванням специфіки обробки персональних даних у різних сферах. **При розробленні такого кодексу поведінки або внесенні змін до нього відповідне об'єднання чи юридична особа може звернутися за висновком до Уповноваженого**». Вказане право є особливо актуальним для володільців, які обробляють особливо великі об'єми персональних даних (зокрема, чутливих категорій персональних даних). В разі якщо порядок обробки персональних даних буде погоджено Уповноваженим це суттєво знижує ймовірність як проведення перевірки, так і констатації порушення. Крім цього, це надає можливість дотримуватися більш однозначної та послідовної позиції в спілкуванні з суб'єктами персональних даних (особливо стосується великих компаній).

Закон та Типовий порядок обробки не визначають, яким чином вказані вище елементи мають бути визначені володільцем (форма та детальність викладу) – в законі/підзаконному акті/установчих/розпорядчих документах, у паперовому чи електронному вигляді. Вирішення цих питань покладається на самого володільця або на закон та залежить від особи володільця (фізична особа, юридична особа приватного/публічного права, державний орган чи орган місцевого самоврядування), кількості та категорій суб'єктів персональних даних, а також категорій персональних даних, що підлягають обробці (загальні, чутливі, профайлинг тощо).

Разом із тим виходячи з актуального стану справ у сфері захисту персональних даних, можна сформувати такі рекомендації з цього приводу.

Якщо обробка здійснюється у зв'язку з необхідністю виконання повноважень, визначених законом, саме законодавство повинне прямо визначати вказані елементи обробки персональних даних.

В залежності від характеру обробки, категорій суб'єктів, складу даних вказані елементи можуть визначатися окремим законом (наприклад, у випадку з Єдиним державним демографічним реєстром)[24]. Підзаконні акти в такому випадку регламентують деталі порядку обробки.

В іншому випадку закон може встановлювати загальні повноваження органу та право збирати персональні дані, а порядок повністю визначається підзаконними актами. Наприклад, відповідно до ст. 25 Закону України «Про національну поліцію», поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ, стосовно, серед іншого, осіб, затриманих за підозрою у вчиненні правопорушень. Під час наповнення цих баз (банків) даних поліція забезпечує збирання, накопичення мультимедійної інформації (фото, відео-, звукозапис) та біометричних даних (**дактилокартки**, зразки ДНК). При цьому така норма встановлює лише загальне право. Для того, щоб в повній мірі відповідати принципу законності більш детальний порядок обробки та захисту дактилоскопічних даних передбачено на разі Інструкцією про порядок функціонування дактилоскопічного обліку експертної служби МВС України, затвердженою наказом МВС України від 11 вересня 2001 року № 785.

Якщо обробка здійснюється приватним суб'єктом (на підставі згоди суб'єкта персональних даних, договору чи для реалізації визначених законом інтересів), він самостійно визначає всі вказані вище елементи обробки персональних даних, які викладає у відповідних установчих, статутних чи інших документах, що регламентують його роботу. **Рекомендовано визначати порядок обробки шляхом прийняття окремого документу (наприклад, політики приватності, кодексу поведінки у сфері захисту персональних**

[24] Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус».

даних тощо), який повинен перебувати у відкритому доступі, зокрема, якщо є така можливість на веб-сайті володільця.

Якщо обробка здійснюється приватним суб'єктом у зв'язку з необхідністю виконання визначених законом обов'язків, закон зазвичай встановлює мету обробки та склад даних. Наприклад, на підставі Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», а також «Про банки та банківську діяльність» визначено об'єм даних, які необхідно збирати банкам з метою ідентифікації клієнтів. Законом України «Про телекомунікації» визначено мету обробки та склад персональних даних, що обробляються у цій сфері операторами, а також загальні зобов'язання щодо захисту цієї інформації. При цьому детальний порядок обробки та захисту такої інформації зазвичай вирішується банками і телекомунікаційними компаніями самостійно. З огляду на об'єми та чутливість персональних даних, що обробляються банками, телекомунікаційними компаніями (іншими великими володільцями), для того, щоб внутрішньо узгодити та уніфікувати процеси обробки персональних даних слід обов'язково впровадити окрему політику приватності.

Разом із тим, якщо обробка здійснюється фізичною особою чи невеликим підприємством, у якого обробка персональних даних не є основним видом діяльності[25] приймати окремий документ немає сенсу. Так, Регламент Європейського Парламенту та Ради передбачає обов'язок володільця/розпорядника вести документацію щодо всіх операцій, пов'язаних із обробкою персональних даних, окрім випадків, коли обробка здійснюється фізичними особами без комерційного інтересу, або підприємством, де працює менше 250 працівників, і обробка є лише додатковим видом його діяльності. Це положення може бути орієнтиром і для національних володільців, а на перспективу може бути імплементоване в національне законодавство.

В разі необхідності порядок обробки та захисту персональних даних можуть бути визначені у кількох документах, наприклад: загальна політика, порядок захисту персональних даних, порядок

[25] Наприклад, усі підприємства обробляють персональні дані своїх працівників та контрагентів, однак такі види обробки не можна віднести до основних видів діяльності, оскільки вони просто супроводжують виконання підприємством своїх основних функцій та завдань.

доступу та роботи працівників володільця з персональними даними тощо.

Якщо володільцем ведеться з різними цілями декілька різних баз персональних даних, він повинен визначити порядок обробки персональних даних щодо кожної з таких баз.

У будь-якому випадку Уповноважений (в разі потреби) та суб'єкти персональних даних (обов'язково) повинні знати про те, що тим чи іншим володільцем здійснюється обробка персональних даних, склад даних та порядок їх обробки. У випадку їх звернення володілець повинен бути готовим невідкладно надати усю інформацію з цього приводу.

ТЕМА 7. ПОРЯДОК ПОВІДОМЛЕННЯ УПОВНОВАЖЕНОГО ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ, ЯКА СТАНОВИТЬ ОСОБЛИВИЙ РИЗИК ДЛЯ ПРАВ І СВОБОД СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ.

Відповідно до ст. 9 Закону, «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, визначаються Уповноваженим. Повідомлення про обробку персональних даних подається за формою та в порядку, визначеними Уповноваженим. Володілець персональних даних зобов'язаний повідомляти Уповноваженого про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого в порядку, визначеному Уповноваженим».

На виконання цього положення Закону Уповноваженим було прийнято Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відпо-

відальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.

Так, відповідно до п. 1.2 Порядку, обробка персональних даних, що становить особливий ризик для прав і свобод суб'єктів – це будь-яка дія або сукупність дій, а саме збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем, яка здійснюється відносно персональних даних про расове, етнічне та національне походження; політичні, релігійні або світоглядні переконання; членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості; стан здоров'я; статеве життя; біометричні дані; генетичні дані; притягнення до адміністративної чи кримінальної відповідальності; застосування щодо особи заходів в рамках досудового розслідування; вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»; вчинення щодо особи тих чи інших видів насильства; місцеперебування та/або шляхи пересування особи.

При цьому відповідно до п. 2.1 володілець персональних даних повідомляє Уповноваженого про здійснення ним будь-яких видів обробки персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, крім випадків, якщо:

1) здійснюється обробка, єдиною метою якої є ведення реєстру для надання інформації населенню, який відкритий для населення в цілому;
2) обробка здійснюється громадськими об'єднаннями, політичними партіями та/або організаціями, професійними спілками, об'єднаннями роботодавців, релігійними організаціями, громадськими організаціями світоглядної спрямованості за умови, що обробка стосується виключно персональних даних членів цих об'єднань та не передається без їх згоди;
3) обробка необхідна для реалізації прав та виконання обов'язків володільця персональних даних у сфері трудових правовідносин відповідно до закону.

Порядком також визначено форму та порядок повідомлення Уповноваженого та порядок оприлюднення Уповноваженим отри-

маної інформації на її офіційному веб-сайті. Статтею 188–39 КУПАП встановлено відповідальність за неповідомлення Уповноваженого впродовж визначених Законом строків (див. Порядок повідомлення Уповноваженого у додатку).

Разом із тим вказана процедура повідомлення в такому вигляді, як вона існує станом на сьогодні, є абсолютно неефективною. *По-перше*, володільці зобов'язані повідомляти Уповноваженого про обробку, **яка вже відбувається**. Тобто, на момент повідомлення Уповноваженого володілець уже організував процес обробки, зібрав певний об'єм персональних даних (обробка яких по суті становить ризик для прав та свобод громадян), вклав певні матеріально-технічні ресурси в організацію процесу обробки. Відтак, якщо організовані володільцем операції з обробки персональних даних містять певні недоліки:

1) права суб'єктів уже порушено і
2) володілець з огляду на прикладені зусилля вже незацікавлений у внесенні змін до операцій з обробки, які ним здійснюються. Тому, і це дуже яскраво прослідковується в реальному часі, володільці намагаються направити повідомлення з якомога загальнішими відомостями, які по суті не надають можливості зробити конкретні висновки щодо операцій, які здійснюються ним.

По-друге, якщо навіть Уповноваженим за результатами аналізу повідомлень буде виявлено обробку, що є незаконною, єдиним результатом буде винесення припису щодо припинення такої обробки або внесення змін до операцій, пов'язаних з обробкою.

По-третє, рівень знання та розуміння законодавства про захист персональних даних в Україні з огляду на новизну його положень є доволі невисоким, що в контексті обов'язку повідомлення Уповноваженого тягне за собою направлення великої кількості помилкових та неправильних повідомлень. Багато хто з володільців не розуміє, чи слід повідомляти, однак про всякий випадок направляє повідомлення. Як наслідок, Уповноваженим вживаються заходи, спрямовані на перевірку отриманої інформації, за результатами яких виявляється, що володільцем просто було допущено помилку. Такі дії не тягнуть за собою відповідальності, однак накладають зайве навантаження на контролюючий орган.

По-четверте, така процедура є вкрай неефективною в контексті роботи державних органів влади. Так, державні органи здійснюють обробку на підставі закону та в порядку визначеному законодавством. В ході розробки проектів відповідних законів та підзаконних нормативно-правових актів, які є підставою чи прямо/опосередковано регламентують порядок обробки персональних даних, у відповідних органів влади відсутнє зобов'язання проводити консультації з Уповноваженим. Відтак, велика частина документів приймається без його відома та часто суперечить Закону. На момент виявлення проблеми Уповноваженим (самостійно чи з повідомлення) обробка вже йде повним ходом і для того, щоб її змінити/припинити необхідно інколи суттєво змінювати закони, що займає дуже багато часу.

Причиною такої ситуації є хибне розуміння авторами Закону сутності процедури повідомлення, яка в дуже спотвореному вигляді була запозичена з Директиви.

У цьому зв'язку варто зазначити, що процедура повідомлення контролюючого органу (або, якщо точніше, попередніх консультацій володільця з контролюючим органом) уже стала звичним явищем серед європейських держав. Так, відповідно до статті 20 Директиви держава повинна визначити операції з обробки даних, які можуть становити певний ризик для прав і свобод суб'єктів персональних даних. Перед **початком таких операцій** контролюючий орган повинен перевірити їх відповідність законодавству про захист персональних даних. Для цього володілець повинен самостійно повідомити контролюючий орган про те, що він планує здійснювати такі операції та узгодити їх порядок. Звідси логічно випливає, що результатом такої перевірки може бути або заборона таких операцій, або видання розпорядження щодо їх модифікації/зміни.

Окремо слід наголосити, що, відповідно до частини третьої вказаної статті Директиви, аналогічні зобов'язання можуть покладатися на «заходи національного парламенту та заходи, які базуються на таких законодавчих заходах». Відтак, як парламент перед прийняттям законів, так і уряд та міністерства перед прийняттям на цій підставі законів, інших нормативно-правових актів зобов'язані забезпечувати їх перевірку контролюючим органом на предмет відповідності Закону та Конвенції. Метою таких положень є недопущення та запобігання можливим порушенням законодавства про захист персональних даних.

Аналогічні та більш детальні правила з цього приводу містяться у статті 34 Регламенту, відповідно до якої у чітко визначених випадках володільці зобов'язані повідомляти наглядовий орган про обробку персональних даних. Якщо на думку наглядового органу, запланована обробка персональних даних суперечитиме Регламенту, він має право заборонити її та надати рекомендації з метою усунення вказаної невідповідності.

ТЕМА 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 Верховної Ради України 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.

ЗАКОН УКРАЇНИ
«ПРО УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ»

Стаття 10. Секретаріат Уповноваженого

Для забезпечення діяльності Уповноваженого утворюється секретаріат, який є юридичною особою, має свій рахунок у банку та печатку встановленого зразка.

Структура секретаріату, розподіл обов'язків та інші питання щодо організації його роботи регулюються Положенням про секретаріат Уповноваженого Верховної Ради України з прав людини (далі – Положення). (...)

Стаття 11. Представники Уповноваженого

Уповноважений має право призначати своїх представників у межах виділених коштів, затверджених Верховною Радою України.

Організація діяльності та межі повноважень представників Уповноваженого регулюються Положенням про представників Уповноваженого Верховної Ради України з прав людини, яке затверджується Уповноваженим.

Наказ Уповноваженого від 27.07.2012 № 7/8–12 «Про затвердження Положення про представників Уповноваженого Верховної Ради України з прав людини».

1. Представники Уповноваженого Верховної Ради України з прав людини (далі – Представник) є посадовими особами, яким з метою здійснення парламентського контролю за додержанням конституційних прав і свобод людини і громадянина делегуються визначені повноваження Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений) та на яких розповсюджуються гарантії забезпечення діяльності Уповноваженого.

Відтак, Представник Уповноваженого з питань захисту персональних даних є посадовою особою, якій делеговано повноваження Уповноваженого у сфері контролю за додержанням законодавства про захист персональних даних, і в тому числі й ті, що стосуються проведення перевірок та прийняття відповідних актів реагування.

СТАТТЯ 23. ПОВНОВАЖЕННЯ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

1. Уповноважений має такі повноваження у сфері захисту персональних даних:

1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

2) проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

3) отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;

(…)

5) за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

6) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або від-

повідальних осіб з організації роботи із захисту персональних даних, інших осіб;

7) взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб;

8) звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

(…)

10) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом.

(…)

Порядок проведення Уповноваженим, його представником та іншими визначеними Уповноваженим службовими особами перевірок 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).

Так, перевірки проводяться Уповноваженим у відповідності до затвердженого ним річного та квартального планів за власною ініціативою або за умови наявності низки інших передбачених Порядком підстав.

ПОРЯДОК ЗДІЙСНЕННЯ УПОВНОВАЖЕНИМ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ КОНТРОЛЮ ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

(…)

3. Проведення планової перевірки

3.1. Планові перевірки проводяться відповідно до річних або квартальних планів, які затверджуються Уповноваженим до 1 грудня року, що передує плановому, або до 25 числа останнього місяця кварталу, що передує плановому.

(…)

4. Проведення позапланової перевірки

4.1. Позапланові перевірки суб'єктів перевірки можуть проводитись за наявності однієї або декількох підстав/приводів, зокрема:

за власною ініціативою Уповноваженого;

при безпосередньому виявленні порушень вимог законодавства про захист персональних даних Уповноваженим, в тому числі і в результаті здійснення дослідження системних проблем щодо забезпечення права на приватність, повагу до приватного та сімейного життя;

при наявності інформації про порушення вимог законодавства про захист персональних даних в повідомленнях, опублікованих в засобах масової інформації, оприлюднених в мережі Інтернет;

обґрунтовані звернення фізичних та юридичних осіб з повідомленням про порушення фізичною особою, фізичною особою – підприємцем, підприємством, установою і організацією усіх форм власності, органом державної влади чи місцевого самоврядування, що є володільцями та/або розпорядниками персональних даних вимог законодавства про захист персональних даних;

виявлення недостовірності у відомостях (даних), наданих суб'єктом перевірки на письмовий запит Уповноваженого щодо здійснення безвиїзної перевірки, та/або якщо такі відомості (дані) не дають змоги оцінити виконання суб'єктом перевірки вимог законодавства про захист персональних даних;

контроль за виконанням суб'єктом перевірки приписів щодо усунення порушень вимог законодавства про захист персональних даних, виданих за результатами проведення перевірок.

(…)

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.

Ці положення зазвичай викликають багато запитань із боку володільців під час проведення перевірок. У зв'язку з цим слід надати пояснення з цього приводу.

Так, відповідно до ч. 4. ст. 5 Закону України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», органи державного нагляду (контролю) здійснюють планові заходи з державно-

го нагляду (контролю) за умови письмового повідомлення суб'єкта господарювання про проведення планового заходу не пізніш як за десять днів до дня здійснення цього заходу.

Відповідно до ч. 3 ст. 6 вказаного Закону суб'єкт господарювання повинен ознайомитися з підставою проведення позапланового заходу з наданням йому копії відповідного документа (наприклад, відповідної скарги).

Згідно з частинами першою та другою статті 7 вказаного Закону для здійснення планового або позапланового заходу орган державного нагляду (контролю) видає **наказ**, який має містити найменування суб'єкта господарювання, щодо якого буде здійснюватися захід, та предмет перевірки. На підставі наказу оформляється **посвідчення** (направлення) на проведення заходу, яке підписується керівником або заступником керівника органу державного нагляду (контролю) (із зазначенням прізвища, ім'я та по батькові) і засвідчується печаткою.

Однак, згідно з преамбулою вказаний Закон визначає правові та організаційні засади, основні принципи і порядок здійснення державного нагляду (контролю) **у сфері господарської діяльності**, **повноваження органів державного нагляду** (контролю), їх посадових осіб і права, обов'язки та відповідальність суб'єктів господарювання під час здійснення державного нагляду (контролю).

Так, відповідно до ч. 1 ст. 3 Господарського кодексу України, під господарською діяльністю розуміємо діяльність суб'єктів господарювання у сфері **суспільного виробництва, спрямовану на виготовлення та реалізацію продукції, виконання робіт чи надання послуг вартісного характеру, що мають цінову визначеність**.

Відповідно до ч. 1 ст. 1 Закону «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» державний нагляд (контроль) – це діяльність уповноважених законом **центральних органів виконавчої влади, їх територіальних органів, державних колегіальних органів, органів виконавчої влади Автономної Республіки Крим, органів місцевого самоврядування** (далі – органи державного нагляду (контролю)) в межах повноважень, передбачених законом, щодо виявлення та запобігання порушенням вимог законодавства суб'єктами господарювання та забезпечення інтересів суспільства, зокрема належної якості продукції, робіт та послуг, допустимого рівня небезпеки для населення, навколишнього природного середовища.

У зв'язку з цим слід наголосити, що відповідно до ст. 1 Закону «Про Уповноваженого Верховної Ради України з прав людини» **парламентський контроль за додержанням конституційних прав і свобод людини і громадянина** та захист прав кожного на території України і в межах її юрисдикції на постійній основі здійснює Уповноважений Верховної Ради України з прав людини (далі – Уповноважений) (...).

Статтею 3 цього Закону передбачено, що метою парламентського контролю, який здійснює Уповноважений, є:

1) захист прав і свобод людини і громадянина, проголошених Конституцією України, законами України та міжнародними договорами України;

2) додержання та повага до прав і свобод людини і громадянина суб'єктами, зазначеними у статті 2 цього Закону;

3) запобігання порушенням прав і свобод людини і громадянина або сприяння їх поновленню;

4) сприяння приведенню законодавства України про права і свободи людини і громадянина у відповідність з Конституцією України, міжнародними стандартами у цій галузі;

5) поліпшення і подальший розвиток міжнародного співробітництва в галузі захисту прав і свобод людини і громадянина;

6) запобігання будь-яким формам дискримінації щодо реалізації людиною своїх прав і свобод;

7) сприяння правовій інформованості населення та захист конфіденційної інформації про особу.

Відповідно до ч. 2 ст. 4 вказаного Закону, **Уповноважений здійснює свою діяльність незалежно від інших державних органів та посадових осіб**.

Частиною першою статті 1 Закону України «Про захист персональних даних» передбачено, що він регулює правові відносини, пов'язані зі захистом і обробкою персональних даних, і **спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя**, у зв'язку з обробкою персональних даних.

Таким чином, по-перше, Уповноважений та працівники Секретаріату в ході перевірок здійснюють контроль за додержанням прав людини, зокрема права особи на невтручання в особисте життя у зв'язку з обробкою персональних даних, а не господарської діяльності підприємства.

По-друге, Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» стосується виключно діяльності «центральних органів виконавчої влади, їх територіальних органів, державних колегіальних органів, органів виконавчої влади Автономної Республіки Крим, органів місцевого самоврядування», до кола яких Уповноважений не належить. Це підтверджується також і гарантіями безсторонності та незалежності, викладеними у Законі України «Про Уповноваженого Верховної Ради України за прав людини».

Тому, Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» не поширюється на перевірки, що проводяться працівниками Секретаріату Уповноваженого.

Відтак, єдиними документами, що регламентують порядок їх проведення, є Закон та Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних.

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

6. ПРАВА ТА ОБОВ'ЯЗКИ УПОВНОВАЖЕНОЇ ПОСАДОВОЇ ОСОБИ ТА ПОСАДОВИХ ОСІБ СУБ'ЄКТА ПЕРЕВІРКИ

6.1. Уповноважена посадова особа при проведенні перевірки має право:

6.1.1. Безперешкодно входити на об'єкт перевірки за службовим посвідченням і мати безперешкодний доступ до місць зберігання інформації, у тому числі й до комп'ютерів, магнітних носіїв інформації тощо.

6.1.2. Отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом.

(…)

6.1.3. Отримувати засвідчені у встановленому законодавством порядку копії документів.

6.1.4. Вимагати в межах своєї компетенції у керівника та/або посадових осіб суб'єкта перевірки надання завірених підписом письмових пояснень.

6.1.5. Звертатись у зв'язку з реалізацією своїх повноважень та відповідно до законодавства до органів прокуратури, інших правоохоронних органів.

6.1.6. Складати та підписувати приписи про запобігання або усунення порушень законодавства про захист персональних даних.

6.1.7. Складати та підписувати протоколи про притягнення до адміністративної відповідальності за виявлені порушення законодавства про захист персональних даних;

6.1.8. Залучати для складання протоколів осіб, присутніх при виявленні правопорушення.

6.2. Уповноважена посадова особа при проведенні перевірки зобов'язана:

6.2.1. Повно, об'єктивно та неупереджено здійснювати перевірку у межах визначених повноважень;

6.2.2. Повідомити керівника суб'єкта перевірки або уповноважену ним особу про свої обов'язки та повноваження, причину та мету перевірки, права, обов'язки керівника та посадових осіб суб'єкта перевірки;

6.2.3. Ознайомити керівника суб'єкта перевірки або уповноважену ним особу з результатами проведеної перевірки та/або протоколом про адміністративні правопорушення;

6.2.4. Визначати перелік необхідних для перевірки документів та строки їх надання;

6.2.5. Належним чином оформлювати результати перевірок;

6.2.6. Неухильно дотримуватись вимог до складання протоколів про адміністративні правопорушення, визначених Порядком оформлення матеріалів про адміністративні правопорушення.

6.3. Посадові особи суб'єкта перевірки, в тому числі керівник суб'єкта перевірки або уповноважена ним особа, під час здійснення перевірки мають право:

6.3.1. Перевіряти наявність в уповноваженої посадової особи (осіб) службового посвідчення та підстав для проведення перевірки;

6.3.2. Бути присутніми під час здійснення перевірки;

6.3.3. Одержувати та ознайомлюватись за результатами проведеної перевірки з Актом та/або протоколом про адміністративне правопорушення;

6.3.4. Надавати в письмовій формі свої пояснення та зауваження до Акта та/або протоколу про адміністративні правопорушення;

6.3.5. Оскаржувати в установленому законом порядку неправомірні дії уповноваженої посадової особи (осіб).

6.4. Посадові особи суб'єкта перевірки, в тому числі керівник суб'єкта перевірки або уповноважена ним особа, під час здійснення перевірки зобов'язані:

6.4.1. Безперешкодно допускати уповноважену посадову особу (осіб) на об'єкт перевірки та надавати доступ до документів та інших матеріалів, потрібних для проведення перевірки;

6.4.2. Надавати необхідні документи, та іншу інформацію, завірені підписом письмові пояснення, а також засвідчені в установленому законодавством порядку копії документів, що необхідні проведення перевірки;

6.4.3. Виконувати вимоги уповноваженої посадової особи (осіб) з питань додержання вимог законодавства про захист персональних даних.

В ході перевірки уповноважені посадові особи 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.

КОДЕКС УКРАЇНИ ПРО АДМІНІСТРАТИВНІ ПРАВОПОРУШЕННЯ

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

Неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей –

тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян.

Невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних –

тягнуть за собою накладення штрафу на громадян від двохсот до трьохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню, –

тягне за собою накладення штрафу на громадян від трьохсот до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових

осіб, громадян – суб'єктів підприємницької діяльності – від п'ятисот до двох тисяч неоподатковуваних мінімумів доходів громадян.

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, –

тягне за собою накладення штрафу на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, –

тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.

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;
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 практично неможливо, 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 передбачає порушення зобов'язання конфіденційності працівниками, залишення робочого місця з незавершеною сесією роботи, передачу особистого паролю доступу іншим особам, відсутність системи ідентифікації користувача перед отриманням доступу до персональних даних, відсутність обліку операцій пов'язаних з обробкою персональних даних, неорганізоване ведення документації (володілець не може підтвердити інформацію про те, чи отримував згоду суб'єкта, чи укладався з ним договір, чи повідомляв суб'єкта про збір його персональних даних та інше), 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. З незаконним доступом усе зрозуміло: якщо вказані вище дії призвели до того, що треті особи незаконно отримали доступ до персональних даних (тобто, без передбачених Законом підстав) значить мало місце правопорушення, передбачене статтею 188–39 КУПАП. На практиці вказана стаття зазвичай **застосовується до ситуацій, коли внаслідок дій працівників володільця треті особи отримують доступ до персональних даних (далі про це йтиме мова більш детально)**.

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).

Насправді будь-яке незаконне поширення/оприлюднення/передача персональних даним третіми особами повинне характеризуватися як правопорушення та тягнути за собою передбачену законом відповідальність.

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.

Далі, 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. Так, станом на сьогодні максимальна штатна структура Управління з питань захисту персональних даних Секретаріату Уповноваженого передбачає 25 співробітників. На перспективу згідно з рекомендаціями експертів кількість працівників планується збільшити до 50 осіб. Разом із тим процедура реєстрації баз персональних даних, яка функціонувала до кінця грудня 2013 року на підставі чинної на той час редакції Закону, показала орієнтовну кількість баз персональних даних в Україні – загалом на реєстрацію було заявлено понад 1,5 мільйона баз персональних даних. Велика частина вказаних заяв є неприйнятними[27]. Незважаючи на це, кількість баз даних величезна в порівнянні зі штатом Управління з питань захисту персональних даних. У зв'язку з цим кожна перевірка працівників Секретаріату, в ході якої було виявлено правопорушення, повинна не лише мати наслідки для володільця-об'єкта перевірки, а й стри-

[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».

[27] Досвід роботи із вказаними заявами показує, що велика кількість заяв подані помилково, з розрахунку краще про всякий випадок подати, ніж не подати і потім можливо мати неприємності. Не більше четвертої частини заяв відповідали вимогам щодо їх реєстрації.

муючий ефект щодо інших володільців. При існуючій системі цього немає. Працівники Секретаріату виносять припис та контролюють його вчасне[28] та повне виконання, що саме по собі може потребувати проведення окремої перевірки. Як наслідок декілька працівників (у перевірках беруть участь не менше двох працівників) вимушені приділяти надто багато часу кожному володільцю.

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

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.

Станом на сьогодні вказані (хоч і не такі значні, як наприклад, незаконне поширення) правопорушення в їх сукупності чи окремо призводять до недоліків функціонування системи захисту персональних даних. Наприклад, навіть якщо очевидно, що персональні дані особи було поширено, відсутність обліку операцій, пов'язаних

[28] Відповідно до ст. 23 Закону строк виконання припису становить не менше 30-ти днів.

з обробкою персональних даних, зазвичай унеможливлює встановлення особи причетної до такого поширення. Особу рідко повідомляють про збір її персональних даних, як наслідок вона і не знає про те, що її персональні дані обробляються новим володільцем, і не направляє скаргу з цього приводу.

Також слід зазначити, що інколи в ході перевірки неможливо встановити конкретну особу, яка причетна до вчинення правопорушення, хоча очевидно, що воно було вчинено конкретним володільцем. Наприклад, медична інформація про особу потрапила у відкритий доступ. До цього така інформація була лише в медичному закладі, де особа проходила лікування. Очевидно, що витік інформації/персональних даних трапився у вказаній лікарні, однак, встановити конкретну особу, відповідальну за незаконне поширення персональних даних неможливо. КУПАП передбачає відповідальність лише фізичних осіб, хоча у цій ситуації стягнення слід накласти саме на юридичну особу. Найчастіше такі питання виникають, коли мова йде про недоліки процесу організації обробки персональних даних володільцем, які базуються на внутрішніх правилах володільця, які інколи є недостатньо чіткими та формальними. Відтак, вкрай необхідно змінити КУПАП в частині щодо можливості накладення стягнення на юридичних осіб. Така практика вже давно присутня в державах Європейського Союзу. Зокрема, в проекті Регламенту викладено чіткий перелік порушень, які тягнуть за собою відповідальність як фізичних, так і юридичних осіб (стаття 79).

Окремо слід наголосити, що передбачені Законом заходи реагування спрямовані на припинення/виправлення порушення законодавства про захист персональних даних та накладення стягнення на особу, відповідальну за його вчинення. Однак, вони не передбачають будь-якого виду компенсації особі, чиї права могло бути порушено вчиненим правопорушенням. При цьому з**а особою залишається право на звернення до суду з позовом про відшкодування шкоди**, завданої порушенням її права на захист персональних даних. У такому випадку основним доказом порушення прав особи буде відповідно припис Уповноваженого або рішення суду за результатами розгляду протоколу про притягнення до адміністративної відповідальності.

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

Це питання є одним із 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.

В Законі є декілька різних термінів, що стосуються надання персональних даних третім особам, а саме доступ (стаття 16 Закону)/поширення та передача (стаття 14 Закону)/передача даних іноземним суб'єктам відносин, пов'язаних із персональними даними (стаття 29 Закону). При цьому надання доступу до персональних даних третім особам та поширення третім особам є фактично одними і тими ж діями (транскордонна передача дещо відрізняється та має свої особливості), які повинні відповідати одним і тим же положенням Закону (див. нижче). Чинна редакція Закону створює враження, що це дві різні процедури, які регламентуються окремо статтею 14 та 16 Закону. Тому видається доцільним при розробці змін до Закону зупинитися на якомусь одному розумінні.

Наприклад, у Директиві «доступ» використовується лише в контексті доступу особи до інформації про себе, коли ж мова йде про третіх осіб використовуються поняття розкриття (шляхом передачі), поширення. Однак, усі вони в Директиві є елементами обробки, до яких застосовуються одні і ті ж правила.

Тим, хто застосовує вказаний Закон, рекомендується виходити з того, що **підстави та правила** передачі персональних даних викладено у статтях 6, 7, 11, 12, 21 Закону. Так, 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 непогано викладає **порядок** доступу третіх осіб до персональних даних. Однак, він стосується лише передачі персональних даних в рамках процедури «запит – відповідь». При цьому

на практиці зустрічаються ще як мінімум два способи передачі персональних даних третім особам – на підставі договору та на підставі положень законодавства, які санкціонують пряму та автоматичну передачу персональних даних (зазвичай між державними органами), щодо яких Закон не встановлює жодних спеціальних вимог. Відтак, слід розглянути можливість доповнення Закону в цій частині. При цьому слід звернути увагу, що міжнародні документи не містять спеціальних норм щодо передачі персональних даних (крім звичайно транскордонної).

Разом із тим процедура «запит-відповідь» є сьогодні найбільш поширеною та супроводжується найбільшою кількістю порушень, а тому її використання слід розглянути більш детально.

По-перше, варто зазначити, що передача персональних даних повинна здійснюватися за згодою особи або на підставі закону (див. розділ щодо принципів обробки, а також частину першу статті 16 Закону). По-друге, вона повинна здійснюватися виключно у випадках, передбачених статями 7 (щодо чутливих даних) та 11 (щодо решти персональних даних) Закону.

ПРАКТИКА ЗАСТОСУВАННЯ ЗАКОНУ УПОВНОВАЖЕНИМ.

До Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений) звернувся заявник зі скаргою на незаконне поширення його персональних даних ОКЗ «_____ обласним клінічним психоневрологічним диспансером» (далі – диспансер).

Так, за словами заявника _____ районний суд (далі – суд) розглядав справу за його позовом до районної 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 та чи було цей діагноз знято станом на травень 2013 року.

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, в рамках якої отримано пояснення керівника диспансеру, який підписав вказану довідку, особи, яка підготувала проект довід-

ки, та особи, яка направила її до суду. Також було отримано посадові інструкції вказаних осіб, копію довідки, що направлялася диспансером, та запит суду. За результатами перевірки було повністю підтверджено факти, викладені заявником, а саме незаконну обробку (поширення) конфіденційної інформації (персональних даних щодо обстежень заявника диспансером та поставлених діагнозів за період з червня 2013 до грудня 2014 року).

Такі дії становлять порушення наведених нижче норм закону:

– Частина шоста статті 6 Закону: *«не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.»*, а також частина друга статті 14 Закону, відповідно до якої *«поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.»*

У даній справі заявник не давав згоди на поширення диспансером його персональних даних за період з червня 2013 до грудня 2014 року. Таке поширення також не було передбачено законом.

Так, суд відповідно до пункту 2 частини четвертої статті 6 Закону України «Про психіатричну допомогу» дійсно має право отримувати від закладів охорони здоров'я на запит інформацію про стан психічного здоров'я заявника. Це підтверджується і частиною другою статті 7 Закону, відповідно до якої дані, що стосуються здоров'я можуть оброблятися, коли це необхідно для обґрунтування, задоволення або захисту правової вимоги.

Однак, у даному випадку 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).

– Частина друга статті 8 Закону *«Суб'єкт персональних даних має право: (...) 7) на захист своїх персональних даних від незаконної обробки (...);»* та частина перша статті 24 Закону *«Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних (...) від незаконної обробки, у тому числі (...) доступу до персональних даних»*.

Згідно з вказаними положеннями володілець зобов'язаний забезпечити захист персональних даних від незаконної обробки, що передбачає з одного боку вжиття активних дій, спрямованих на запобігання незаконній обробці персональних даних, а з іншого – утримуватися від дій, що становлять незаконну обробку.

Останнє зобов'язання деталізується частиною третьою статті 10 Закону, відповідно до якої *«Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники 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, крім випадків, передбачених законом.».

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 містять, 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, керуючись пунктом 10 частини першої статті 23 Закону (*«Уповноважений має такі повноваження у сфері захисту персональних даних: (...) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;»*), 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 до інформаційно-аналітичного відділу Департаменту, 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. При подачі списку, файл називати відповідно до назви території, яка подає інформацію*» (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, части-

ни 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.

Вказані дії були достатньою підставою для складення адміністративного протоколу та направлення його до суду для вирішення питання щодо притягнення керівника медичного закладу до відповідальності. Однак, з огляду на те, що на момент виявлення правопорушення минули строки накладення адміністративного стягнення та провадження підлягало закриттю, Уповноваженим було надано роз'яснення щодо недопущення в майбутньому схожих правопорушень та припис щодо видалення незаконно накопиченої інформації про пацієнтів.

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. Наприклад, Правління Національного Банку України прийняло постанову від 14.07.2006 № 267 «Про затвердження правил зберігання, захисту, використання та розкриття банківської таємниці», у якій визначило порядок оформ-

лення та розгляду запитів про надання доступу до банківської таємниці. Більш детально це питання розглядалося Уповноваженим. Це можна проілюструвати на прикладі, який розглядався нами раніше (див. нижче).

ПРАКТИКА ЗАСТОСУВАННЯ ЗАКОНУ УПОВНОВАЖЕНИМ.

До Уповноваженого надійшла скарга заявника щодо відмови надати йому інформацію про особу, що робила щеплення його дитині, через ненадання 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 з 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, в разі 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, виходячи із вищевказаного, для отримання запитуваної інформації про доньку, заявнику у своєму запиті до Київського міського пологового будинку №1 необхідно 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.

Відтак, 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 випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до них.

Крім цього, відповідно до ч. 3 ст. 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, крім випадків, передбачених законом.

З цією метою володілець персональних даних повинен вжити розумних заходів, спрямованих на забезпечення захисту прав 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**.

Відтак, 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 з 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 витребовування разом із запитом копії сторінки документа, що посвідчує особу, яка містить особистий підпис запитувача (наприклад, паспорт), що необхідно для здійснення верифікації (встановлення справжності підпису шляхом візуального порівняння зі зразком).

Крім 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.

Також є певні особливості надання доступу третім особам до інформації (персональних даних) в рамках Закону України «Про доступ до публічної інформації» (де запитувачі інформації – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень, а розпорядники інформації – суб'єкти, визначені у статті 13 Закону[29]).

ПРАКТИКА ЗАСТОСУВАННЯ ЗАКОНУ УПОВНОВАЖЕНИМ.

Відповідно до Закону України «Про доступ до публічної інформації», публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом. Тобто, персональні дані, які знаходяться у володінні суб'єктів владних повноважень та інших розпорядників публічної інформації належать до публічної інформації.

Один із принципів доступу до публічної інформації, визначених статтею 4 Закону України «Про доступ до публічної інформації», є вільне отримання та поширення інформації, крім обмежень, встановлених законом.

Порядок надання публічної інформації залежатиме від того, чи належить запитувана інформації (і в тому числі персональні дані) до інформації з обмеженим доступом чи ні.

[29] 1. Розпорядниками інформації для цілей цього Закону визнаються:

1) суб'єкти владних повноважень – органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

2) юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, – стосовно інформації щодо використання бюджетних коштів;

3) особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, – стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

(…)

2. До розпорядників інформації, зобов'язаних оприлюднювати та надавати за запитами інформацію, визначену в цій статті, у порядку, передбаченому цим Законом, прирівнюються суб'єкти господарювання, які володіють:

(…)

4) іншою інформацією, що становить суспільний інтерес (суспільно необхідною інформацією).

Загальні положення.

Прийняття рішення щодо обмеження доступу до інформації повинне кожного разу (зокрема, у зв'язку з розглядом кожного запиту) базуватися на застосуванні передбаченого статтею 6 Закону України «Про доступ до публічної інформації» «трискладового» тесту, відповідно до якого доступ до інформації може бути обмежено у разі дотримання 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.

Якщо така інформація, включаючи персональні дані, не належить до інформації з обмеженим доступом, вона надається будь-якому визначеному ст. 13 Закону України «Про доступ до публічної інформації» запитувачу інформації незалежно від способу подання запиту – в усній, письмовій чи іншій формі (поштою, факсом, телефоном, електронною поштою) на вибір запитувача.

Якщо розпорядник дійшов висновку, що запитувана інформація, наприклад, персональні дані, є конфіденційною (тобто такою, що може поширюватися лише за згодою особи або у випадках, передбачених законом) вирішення питання щодо надання до неї доступу залежить від того, чи запитує її суб'єкт персональних даних, чи треті особи.

Щодо запитів третіх осіб.

Доступ третіх осіб залежатиме від наявності у них законних підстав для цього, а саме згоди суб'єкта персональних даних або норми закону.

За наявності таких підстав запитувана інформація надається за умови дотримання вимог статті 16 Закону України «Про захист персональних даних» стосовно змісту запиту, зокрема, у запиті має бути зазначено:

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.

Саме інформація, надана запитувачем відповідно до останнього пункту запиту, дозволить володільцю персональних даних прийняти рішення щодо права третьої особи на доступ до персональних даних.

Якщо 1) володільцем не виявлено законних підстав для надання третій особі доступу до персональних даних суб'єкта (згоди або норми закону); 2) такі підстави не вказано у запиті; або 3) відсутні відомості достатні для того, щоб ідентифікувати особу запитувача (зокрема у випадку недотримання положень статті 16 Закону), така інформація (персональні дані) не надається.

Щодо запитів суб'єкта персональних даних.

Відповідно до статті 10 Закону України «Про доступ до публічної інформації», розпорядники інформації, які володіють інформацією про особу, зобов'язані надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом.

Відповідно до частини сьомої статті 16 Закону України «Про захист персональних даних», суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання прізвища, ім'я та по батькові, місця проживання (місце перебування) і реквізитів документа, що посвідчує фізичну особу, яка подає запит. При цьому звертаємо увагу, що законодавством не передбачено обов'язку суб'єкта персональних даних зазначати мету доступу до власних персональних даних.

Також суб'єкт персональних даних має вжити розумних та необхідних заходів щодо підтвердження своєї особи (зокрема, вказавши викладену в частині сьомій статті 16 Закону інформацію), оскільки виключно «суб'єкт» користується безперешкодним доступом до своїх персональних даних (щодо ідентифікації особи запитувача мова йшла вище).

ТЕМА 10. ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ.

1. Посилення спроможності наглядового органу щодо захисту персональних даних у світовій мережі.

Станом на сьогодні незаконне поширення персональних даних у мережі Інтернет залишається практично безкарним. Так, особу, яка поширила персональні дані, як правило, просто неможливо встановити, оскільки доменне ім'я сайту, де незаконно поширені персональні дані, зареєстроване зазвичай в іншій державі. Більше того, інформація, надана хостинг-провайдером щодо особи, яка зареєструвала доменне ім'я, також не завжди відповідає дійсності.

В інших державах у таких випадках є можливість заблокувати доступ до веб-сторінки чи видалити її. Для цього наглядовий орган спочатку звертається до адміністрації сайту з вимогою (приписом) видалити інформацію, що порушує права суб'єкта на захист персональних даних. У випадку відсутності реакції наглядовий орган або самостійно блокує доступ до сторінки, де містяться незаконно поширені персональні дані, або звертається з цією метою до суду, який приймає відповідне рішення. При цьому, якщо наглядовий орган здійснює блокування самостійно, особа, яка розмістила відповідну інформацію на веб-сайті має право оскаржити такі дії до суду.

В Україні станом на сьогодні відсутні будь-які юридичні механізми такого характеру. Як наслідок, ні встановити особу, яка причетна до незаконного поширення інформації, ні заблокувати доступ до такої інформації немає можливості.

При цьому усвідомлюючи такий стан справ, правопорушники часто навіть не намагаються приховати незаконність розміщеної інформації. Звісно, надання таких повноважень наглядовому органу може призвести до суперечливих ситуації, коли адміністрація сайту вважатиме, що розміщена інформація не порушувала законодавство, а наглядовий орган доводитиме протилежне. Однак, саме для цього такі повноваження наглядового органу повинні здійснюватися під попереднім чи ретроспективним контролем суду. Таким чином, буде врівноважено право особи на захист її приватного життя та право адміністрації сайту на свободу висловлення поглядів та поширення інформації.

На даний час абсолютна безкарність поширення інформації в Інтернеті призводить до частих порушень права особи на приватність і відповідальність за такий стан справ повністю лежить на державі.

В якості прикладів вказаного порушення є поширення в Інтернеті інформації про працівників правоохоронних органів, вболівальників, активістів та журналістів під час Майдану, про членів добровольчих батальйонів, осіб, які начебто ухиляються від служби в армії, осіб, які на думку адміністрації сайту, схильні до сепаратизму (веб-сайт «Миротворець»). У деяких випадках поширення інформації може нести загрозу життю тих, кого вона стосується, в інших – така інформація є нічим непідтвердженою, а тому часто неправдивою.

Таким чином, на законодавчому рівні слід передбачити механізм блокування розміщеної в Інтернеті інформації. Це буде корисно не лише в цілях захисту персональних даних, а й в цілях захисту авторського права та національної безпеки. Слід чітко визначити органи, які прийматимуть рішення щодо блокування контенту (Уповноважений у частині персональних даних, СБУ в частині захисту національної безпеки та ін.), контролюватимуть законність таких рішень (суди) та фактично виконуватимуть вказані рішення (наприклад, Державна служба спеціального зв'язку та захисту інформації України).

2. **Чітке визначення того, як співвідносяться поняття «конфіденційна інформація» та «персональні дані».**

На нашу думку (див. третій розділ) стаття 5 Закону потребує концептуальних змін, якими необхідно встановити, що персональні дані є конфіденційною інформацією і їх обробка здійснюється виключно на підставі статей 7 та 11 Закону України «Про захист персональних даних».

3. **Необхідно впорядкувати статті 7 та 11 Закону, які є одними з його ключових положень**, а саме привести їх у відповідність до Директиви та проекту Регламенту. У цих двох документах вони практично не відрізняються за змістом та охоплюють усі допустимі випадки обробки персональних даних. Виклад цих статей вже став типовим і не потребує жодних корекцій.

Перш за все мова йде про такі підстави обробки персональних даних як необхідність реалізації законного інтересу, необхідність виконання повноважень передбачених законом, обробка чутливих даних у цілях охорони здоров'я, які як вже було сказано вище у роз-

ділі щодо підстав обробки, викладені в тексті Закону зі суттєвими упущеннями.

4. У Законі слід надати більш чітке визначення згоди на обробку персональних даних.

У статті 2 Закону надано визначення поняття «згода», де вказано, що передумовою її надання є «поінформованість» суб'єкта персональних даних. У цьому випадку така «поінформованість» передбачає виконання володільцем персональних даних положень статті 12 Закону (яка визначає порядок збирання персональних даних) щодо надання суб'єкту персональних даних завчасно інформації, необхідної для прийняття рішення про надання згоди на обробку його персональних даних. Проте, це явно не визначено у Законі.

Крім цього, у Законі слід прямо визначити, що тягар доведення того, що суб'єкт надав згоду на обробку персональних даних лежить саме на володільці.

5. Щодо використання персональних даних.

Стаття 10 Закону, якою визначається порядок використання персональних даних володільцем, потребує уточнення, оскільки окремі положення цієї статті недостатньо чіткі.

По-перше, слід узгодити між собою поняття використання, обробки та захисту, про що мова йшла у розділі першому. Потрібно також чітко вказати, що використання даних є окремим елементом обробки, в той час як захист окремим та незалежним від обробки поняттям.

Частиною другою статті 10 Закону передбачено, що «використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними».

Друге речення цієї частини взагалі є незрозумілим, а тому його слід видалити. Крім цього, ця норма потребує доповнення. Зокрема, необхідно передбачити обов'язок володільця **фіксувати, хто (з працівників), з якого часу та в якому об'ємі користується доступом до персональних даних, а також коли та кого було позбавлено такого доступу**.

Потрібно ввести окреме положення до закону, яким зобов'язати володільця та розпорядника персональних даних вести облік опе-

рацій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них, та з цією метою зберігати інформацію про те, **хто (зокрема, з працівників чи ін.), коли та з якою метою здійснював збір, зміну, перегляд, передачу (у такому випадку кому), видалення (знищення) персональних даних**.

6. **Щодо компетенції Уповноваженого у сфері захисту персональних даних.**

В цій частині слід чітко визначити:

- що права Уповноваженого стосуються також його представників чи представника з питань захисту персональних даних та визначених працівників Секретаріату Уповноваженого;
- строк надання відповідей на запити Уповноваженого (не більше 10 днів або ж обумовити його вказівками наданими Уповноваженим), оскільки станом на сьогодні строк розгляду запиту Уповноваженого щодо надання доступу до персональних даних є таким як і для всіх – 30 днів відповідно до ст. 16 Закону;
- право доступу Уповноваженого та визначених ним працівників Секретаріату за посадою до інформації з обмеженим доступом і в тому числі персональних даних, службової, таємної інформації (необхідне для здійснення контролю за додержанням законодавства про захист персональних даних у сфері правоохоронної діяльності, зокрема за правильністю обробки інформації отриманої в ході оперативно-розшукової діяльності та негласних слідчих дій. Станом на сьогодні ці сфери є абсолютно безконтрольними) та інформації, що містить банківську таємницю (найбільша кількість скарг щодо незаконної обробки персональних даних надходить власне щодо банків, які у великій кількості випадків відмовляються надавати інформацію, посилаючись на законодавство про банківську таємницю). Відповідно слід змінити низку інших законів, зокрема Закон України «Про банки та банківську діяльність»;
- право Уповноваженого за власним рішенням блокувати доступ до інформації, розміщеної в Інтернеті (див. вище);
- окреме право здійснювати контроль за ходом обробки та захисту інформації в ході проведення оперативно-розшукової діяльності та негласних слідчих дій;

Слід розглянути можливість передачі розгляду справ про порушення законодавства про захист персональних даних Уповноваженому.

7. **Необхідно реформувати систему повідомлення (див. вище відповідний розділ).**

У Законі потрібно чітко вказати, що володільці, які здійснюють обробку персональних даних, що становить ризик для прав та свобод суб'єктів, повинні завчасно про це повідомляти Уповноваженого, а також про порядок такої обробки. Обробка не може розпочинатися до того, як буде отримано погодження Уповноваженого. Закон повинен також передбачати визначення того, що є обробкою, яка становить ризик для прав та свобод суб'єктів персональних даних.

8. **У Законі необхідно переглянути випадки, коли визначається структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці.**

Крім того, необхідно детально викласти у Законі завдання та повноваження такої особи (див. основні напрямки діяльності та права відповідальної особи у відповідному розділі вище).

Також необхідно викласти вимоги, які ставляться до такої особи чи керівника відповідного підрозділу, зокрема щодо наявності відповідних знань у сфері захисту персональних даних.

9. **Передбачений Законом обов'язок володільця повідомляти про збір персональних даних повинен містити винятки зі загального правила** (див. вище відповідний розділ). При цьому слід прибрати з Закону обов'язок володільця повідомляти про дії з персональними даними, видалення персональних даних та ін..
10. **Закон повинен не лише перелічувати права особи, а й містити більш детальні положення щодо порядку їх реалізації.** Так, у відповідному розділі вище мова йшла щодо необхідності деталізації положень про доступ суб'єкта до персональних даних, порядку розгляду вимог щодо видалення та зміни персональних даних, порядку повідомлення про механізми обробки та прийняття автоматизованого рішення, підстави та порядок видалення персональних даних володільцем.
11. **Підстави обмеження дії Закону, що передбачені статтею 25, повинні бути більш детальними в частині, що стосується суспільно необхідних цілей такого обмеження.**

Станом на сьогодні таких цілей тільки три. Лише при дуже широкому тлумаченні вони передбачають всі необхідні випадки обмеження дії визначених норм Закону(стаття 6, 7 та 8).

12. **Поширення персональних даних та надання доступу до персональних даних.** Норми щодо поширення на накопичення персональних даних слід видалити, оскільки перші є очевидними (у Законі є вичерпний перелік підстав обробки персональних даних (статті 7 та 11), які стосуються також і поширення, як одного з елементів обробки), а другі не мають жодної регуляторної сили (стаття 13 Закону містить лише визначення понять накопичення та зберігання, які слід або видалити, або перенести у статтю 2 Закону до решти визначень).
13. **Слід розмежувати/впорядкувати визначення понять доступу та передачі/розкриття/поширення/оприлюднення.** У всіх міжнародних документах доступ стосується лише суб'єкта персональних даних, розкриття – отримання в будь-якій формі персональних даних третьою особою в межах юрисдикції однієї держави, а передача вживається виключно з епітетом транскордонна.
14. **Необхідно узгодити Закон та Закон України «Про доступ до публічної інформації».** В принципі при уважному прочитанні обох законів цього робити не потрібно. Так, стаття 11 Закону, яка містить вичерпний перелік підстав обробки і в тому числі поширення персональних даних. Коли мова йде про необхідність надання державним органом відповіді на запит про доступ до публічної інформації чи оприлюднення такої інформації, це охоплюється такою підставою обробки персональних даних як «необхідність виконання визначених законом повноважень». Коли мова йде про необхідність юридичної чи фізичної особи надавати інформацію на запит, це охоплюється підставою щодо «необхідності виконання передбачених законом обов'язків».

Однак, з огляду на те, що відмова в наданні публічної інформації часто безпідставно обґрунтовується наявністю серед запитуваної інформації персональних даних, слід у статті 11 (а відтак ймовірно і статті 7 Закону) окремо зазначити, що надання доступу до публічної інформації, яка містить персональні дані, повинне здійснювати-

ся в порядку/з урахуванням (статті 6) Закону України «Про доступ до публічної інформації».

15. Слід більш детально врегулювати відносини між володільцем та розпорядником.

Питання взаємодії володільця персональних даних та розпорядника персональних даних мають бути врегульовані окремою статтею Закону, де буде визначено наступне:

1. Спосіб взаємодії – закон або договір.
2. Порядок розподілу відповідальності між володільцем та розпорядником персональних даних. Розпорядник здійснює обробку виключно в рамках вказівок, наданих володільцем. Всі вказівки повинні бути задокументованими.
3. Вимоги до договорів між володільцем і розпорядником персональних даних:
   - предмет та строк дії договору;
   - мета обробки персональних даних;
   - склад персональних даних та категорії суб'єктів персональних даних, що обробляються розпорядником;
   - визначення вимог до технічних та організаційних заходів захисту в ході обробки цих даних розпорядником;
   - покладення на володільця відповідальності перед суб'єктом персональних даних, зокрема за дії розпорядника під час обробки його даних. Саме володілець несе відповідальність перед суб'єктом, доки не доведе, що порушення прав суб'єкта сталося з вини розпорядника;
   - можливість (право) розпорядника залучати субпідрядників до процесу обробки персональних даних;
   - процедура видалення та знищення персональних даних розпорядником, у тому числі внаслідок закінчення строку дії договору (чи через певний час після цього), та повернення володільцю носіїв персональних даних;
   - перенесено положення частин 2–5 статті 4 Закону, з урахуванням вищезазначених змін до них та з деталізацією особливостей залучення розпорядника, коли володільцем персональних даних є орган державної влади чи місцевого самоврядування.

4. Володілець перед укладенням договору та в подальшому контролює відповідність обробки персональних даних розпорядником умовам договору та законодавству.

16. Передбачений пунктом 2 частини 4 статті 29 Закону випадок, коли персональні дані можуть передаватися іноземним суб'єктам відносин, пов'язаних із персональними даними (*а саме: необхідність укладення чи виконання правочину між володільцем персональних даних та* ***третьою особою – суб'єктом персональних даних на користь суб'єкта персональних даних****),* викладений некоректно, а тому потребує уточнення та приведення у відповідність до положень міжнародно-правових актів.

17. Щодо вдосконалення процедури притягнення до відповідальності за порушення законодавства про захист персональних даних.

По-перше, слід видалити частину четверту статті 188–39 (про це мова йшла вище) та передбачити натомість відповідальність за окремі порушення положень Закону. Слід також розширити межі санкцій та залишити це питання на розсуд органу, що виносить рішення про притягнення до відповідальності. При цьому, найнижчий поріг слід починати з попередження. Так, у практиці Уповноваженого траплялися випадки, коли володільцем було незаконно поширено відомості щодо однієї особи (інформація щодо одного поставленого діагнозу). З одного боку, це чутлива інформація, а з другого – лише щодо однієї особи. Мінімальний штраф за таке правопорушення становить 100 неоподаткованих мінімумів (1700 грн.), що є очевидно надмірним покаранням.

По-друге, запровадити відповідальність юридичних осіб (див. розділ щодо контролю за додержанням законодавства про захист персональних даних).

По-третє, продовжити строк притягнення до адміністративної відповідальності та накладення стягнення. Так, станом на сьогодні такий строк становить 3 місяці. За цей час особа повинна встигнути направити скаргу, Уповноважений розглянути її, зібрати матеріали, оформити правопорушення (зокрема скласти протокол), ознайомити з матеріалами правопорушника, направити матеріали до суду, а суд розглянути справу. Зазвичай вже суб'єкт направляє скаргу із запізненням (часто навіть після закінчення трьохмісячного строку). Від-

так доцільно продовжити строки притягнення до відповідальності та накладення стягнення за порушення законодавства про захист персональних даних до 1 року. Зазначене є актуальним навіть якщо право виносити постанови у справах про порушення законодавства про захист персональних даних буде передано Уповноваженому.

По-четверте, в законодавстві слід передбачити обов'язкову участь представників Уповноваженого в ході розгляду питань про притягнення до відповідальності за порушення законодавства про захист персональних даних. Незалежно від того, чи розглядати справу про порушення законодавства про захист персональних даних та виносити по ній рішення будуть суди, чи Уповноважений (а представники володільця оскаржуватимуть рішення до суду), представники Уповноваженого повинні бути учасниками судового процесу. Це необхідно і з тих міркувань, що Закон є доволі новим, практики мало, а рівень його розуміння навіть серед суддів не є на належному рівні.

18. Крім цього вкрай необхідним є впорядкування положень статті 6 Закону. У цій статті викладено ключові принципи обробки персональних даних, які, як ішлося вище, є ключовими зобов'язаннями кожного володільця в ході здійснення ним обробки персональних даних. Лише у виключних випадках допускаються відступи від їх положень (див. розділ щодо обмеження дії принципів вище). Однак, деякі з вказаних принципів викладено невірно чи недостатньо чітко.

Наприклад, чітке визначення принципу законності взагалі відсутнє. В загальних рисах його викладено в частині п'ятій статті 6 Закону: «Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством». Однак, у вказаному положенні мова йде все-таки про мету обробки (її визначеність за згодою особи або на підставі закону), а не обробку як таку. Є й інше положення: «Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». Виходячи з цього положення, складається враження, що обробка на підставі згоди або закону стосується лише персональних даних, які є конфіденційною інформацією. **Це невірне розумін-**

ня. Принцип законності стосується всіх персональних даних. Так, персональні дані (всі категорії персональних даних) обробляються виключно за згодою особи або на підставі закону. Більш детально принцип законності викладено у статтях 7 та 11 Закону. Таке розуміння є єдиноправильним.

ТЕМА 11. ТЕНДЕНЦІЇ РОЗВИТКУ СВІТОВОЇ ТА ЄВРОПЕЙСЬКОЇ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.

МОДЕРНІЗАЦІЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Правила захисту персональних даних, які застосовуються в Європі, встановлені двома міжнародними інструментами. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних бере початок з 1981 року і була першим міжнародним документом, який встановив юридично обов'язкові правила захисту персональних даних. Більшість європейських країн, включаючи Україну, є сторонами цього документу. Конвенція була доповнена в 2001 році Додатковим протоколом, який встановлює правила щодо органів нагляду та транскордонних потоків даних. Держави-члени Європейського Союзу також мають зобов'язання відповідно до Директиви ЄС «Про захист прав приватних осіб стосовно обробки персональних даних та про вільний рух таких даних» 1995 р., яка містить у цілому схожі, але більш детальні положення, у порівнянні з Конвенцією. Відбувся швидкий розвиток інформаційних та комунікаційних технологій із часу прийняття цих інструментів і, відповідно, в даний час ведеться робота і Радою Європи, і Європейським Союзом із метою зробити їх інструменти з питань захисту персональних даних більш придатними до реагування на виклики двадцять першого століття.

Рада Європи

Підхід Ради Європи – внести зміни до чинної Конвенції, замість того, щоб створювати новий документ. У цьому процесі досягнуто значного прогресу, хоча вінце не завершений. Підготовлений проект змін включатиме положення з Додаткового протоколу в тек-

сті самої Конвенції, а також буде мати велику кількість поправок. Це збереже основні принципи, навколо яких ґрунтується існуюча система, але будуть введені деякі нові важливі положення. Надання вичерпного переліку усіх новел виходить за рамки цієї роботи, але наступні нововведення є серед тих, що пропонуються:

- новий принцип захисту персональних даних, що вимагає, щоб процес обробки був пропорційним і служив досягненню балансу між інтересами володільців і прав фізичних осіб;
- запровадження окремого положення, яке встановлює законні підстави для обробки;
- включення в категорію «чутливих персональних даних» генетичних і біометричних даних, які унікальним чином ідентифікують особу, а також посилення гарантій щодо обробки чутливих категорій персональних даних;
- покладання нового зобов'язання на володільців персональних даних повідомляти контролюючий орган про серйозні порушення правил захисту персональних даних;
- передбачення вимоги для володільців надавати визначену інформацію особам, чиї персональні дані зібрані;
- деякі додаткові права для фізичних осіб і нові обов'язки для володільців;
- переглянуто заходи щодо регулювання передачі персональних даних в інші країни;
- посилені повноваження контролюючих органів.

Європейський Союз

У відповідь на нове технологічне середовище, Європейська комісія підготувала проект нового Регламенту, щоб замінити існуючу Директиву[30], оскільки існують відмінності в тому, яким чином держави-члени виконують Директиву. Комісія бачить необхідність більшої узгодженості, отже Регламент матиме пряму дію в державах-членах. Проект був ретельно переглянутий Європейським парламентом та Радою міністрів (представленою державами-членами), які запропонували багато поправок. Комісія, Парламент і Рада в даний час обговорюють проект спільно з метою спробувати досягти згоди щодо тексту.

[30] Комісія також підготувала проект Директиви щодо захисту персональних даних, коли особисті дані обробляються в правоохоронних цілях. Цей проект Директиви не розглядається тут.

Нижче наводяться деякі з основних змін, запропонованих Комісією. Проте, жодних гарантій, що ці зміни будуть включені до тексту документу немає, оскільки він ще потребує тристоронніх обговорень та узгодження:

- розширене визначення суб'єкта персональних даних. Нове визначення передбачає можливість ідентифікації суб'єкта за допомогою, серед іншого, визначення його місця перебування (шляхів пересування), розумових, фізіологічних, генетичних, економічних та інших особливостей. Наприклад, постійно спостерігаючи шляхи пересування особи (за допомогою, наприклад, мобільних додатків), можна виявити її особливості, звички, які дають можливість безпомилково ідентифікувати її серед інших, хоч у володільця таких даних і немає її особистих даних;
- обмеження на використання згоди у якості законної підстави для обробки, а також деталізація її визначення. Так, згідно з Регламентом згода повинна бути чіткою, конкретною та поінформованою;
- необхідність обов'язкового документального підтвердження згоди володільцем;
- включення деяких спеціальних положень, що стосуються дітей (наприклад, запроваджено особливі вимоги до обробки персональних даних дітей, зокрема тих, які не досягли 13-річного віку);
- включення генетичних даних у категорію «чутливі персональні дані», а також визначення понять генетичних, біометричних даних та даних про стан здоров'я;
- введено поняття та надано визначення головного офісу володільця та інше;
- деталізовано основні принципи обробки персональних даних, зокрема принцип пропорційності, окремо викладено принципи прозорості (транспарентності) та підзвітності;
- деякі зміни в процедурах для введення в дію прав фізичних осіб;
- значне збільшення обсягу інформації, що надається особам, чиї персональні дані збираються;
- зобов'язання про те, що повідомлення про обробку володільцем суб'єкта здійснюється простою та доступною мовою;

- деталізація положень щодо повідомлення суб'єкта про обробку його персональних даних та наслідків ненадання персональних даних суб'єктом;
- введення «права бути забутим»[31];
- нове право передачі даних, що дає право особам передавати свої персональні дані з однієї електронної системи (і одного володільця) до іншої;
- нова вимога для володільців персональних даних щодо реалізації «захисту персональних даних за конструкцією» і «захисту персональних даних за замовчуванням»[32] (data protection by design and by default). Відповідно до частини першої статті 23 проекту Регламенту в залежності від сфери діяльності та вартості імплементації володілець як під час визначення засобів обробки, так і в ході її здійснення зобов'язаний вживати необхідних технічних та організаційних заходів для того, щоб обробка відповідала Регламенту (data protection by design). Згідно з частиною другою статті 23 проекту Регламенту передбачає, що володілець зобов'язаний імплементувати механізми гарантування того, що за умовчанням 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 (data protection by default);
- запроваджено поняття профайлингу, визначено допустимі випадки для його застосування та необхідні для цього умови;
- посилення відповідальності розпорядників. Крім цього, Регламентом запроваджено детальні положення щодо регламентації відносин між володільцем та розпорядником. Так, Регламент встановлює низку обов'язкових вимог до догово-

[31] Рішення Європейського Суду від 2014 року у справі «Google Іспанії проти Google Inc» означає, що право вже існує, але чинна Директива прямо його не закріплює.

[32] Передбачають вимоги до володільців щодо прийняття відповідних технічних та організаційних заходів для посилення захисту персональних даних як при розробці системи обробки захисту персональних даних, так і під час самої обробки забезпечити, щоб, за замовчуванням, передбачався мінімальний ризик для фізичних осіб.

ру, що укладається між володільцем та розпорядником, а також зобов'язує документувати результати їх взаємодії;

- скасування вимоги для розпорядників повідомляти контролюючий орган про обробку персональних даних, яку вони здійснюють, що, своєю чергою, замінюється вимогою кращого документування процесів, пов'язаних із обробкою персональних даних, розпорядниками;
- нова вимога для розпорядників повідомляти контролюючий орган та суб'єкти персональних даних, щодо яких порушуються правила обробки персональних даних. При цьому Регламент встановлює мінімальні вимоги щодо змісту таких повідомлень, умов та строків їх направлення;
- детальні положення щодо проведення оцінки можливого впливу операцій із обробки на захист персональних даних (у яких випадках та яким чином вона здійснюється) та проведення консультацій із наглядовим органом, зокрема з метою погодження з ним процедур, пов'язаних з обробкою персональних даних;
- нова вимога для деяких володільців призначати відповідальних осіб (офіцерів) зі захисту персональних даних. Регламент, зокрема, встановлює вимоги до посад офіцерів з питань захисту персональних даних, вимоги до кандидатів, мінімальний перелік їх повноважень та випадки, коли посада офіцера має бути обов'язково запровадженою володільцем;
- вимоги до кодексів обробки персональних даних;
- право суб'єктів оскаржувати дії або бездіяльність наглядового органу, а також у якості альтернативи скарзі до наглядового органу звертатися до суду;
- нове положення для контролюючих органів щодо співпраці у випадках, коли обробка персональних даних відбувається в більше, ніж одній країні-учасниці, й один із контролюючих органів бере на себе ініціативу ведучого процесом («одне вікно»);
- створення нової Ради зі захисту персональних даних на заміну існуючій відповідно до статті 29 Робочій групі зі захисту фізичних осіб при обробці персональних даних («Робоча група статті 29»);
- детальний перелік порушень Регламенту, які тягнуть за собою відповідальність у вигляді попередження та штрафу, а

також граничні розміри штрафів щодо кожної з визначених груп порушень. Так, згідно з Регламентом максимальний розмір штрафу, що може бути накладено на володільця становить до 1 000 000 євро, а у випадку підприємства – до 2 % від річного світового обороту підприємства.

Загалом слід зазначити, що вказаний документ закріплює в основному існуючу практику застосування законодавства про захист персональних даних в Європі. Його положення спрямовані на гарантування того, що кожен суб'єкт зможе здійснювати повний контроль над обробкою його персональних даних у сферах, що охоплюються Регламентом.

Проект Регламенту враховує усі останні тенденції в системі захисту персональних даних в Європі і світі та повинен станом на сьогодні слугувати дороговказом щодо шляхів реформування національного законодавства у сфері захисту персональних даних.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Поняття «персональні дані», його нормативне визначення.
2. Джерела правового регулювання захисту персональних даних: міжнародні та національні нормативно-правові акти.
3. Закон України «Про захист персональних даних» як основний документ у сфері захисту персональних даних в Україні.
4. Класифікація персональних даних.
5. Поняття та види обробки персональних даних.
6. Суб'єкти відносин із захисту персональних даних.
7. Володілець персональних даних та його правовий статус.
8. Розпорядник персональних даних та його правовий статус.
9. Треті особи та одержувач як суб'єкти правовідносин із захисту персональних даних.
10. Уповноважений Верховної Ради з прав людини як суб'єкт правовідносин із захисту персональних даних.
11. Поняття та види принципів обробки персональних даних.
12. Закріплення принципів обробки персональних даних у законодавстві України.
13. Принцип законності обробки персональних даних.
14. Принцип визначеності мети обробки персональних даних.
15. Особливості обробки персональних даних в історичних, наукових та статистичних цілях відповідно до принципу визначеності мети обробки.
16. Принцип адекватності, ненадмірності та пропорційності обробки персональних даних.
17. Принцип достовірності та точності обробки персональних даних.
18. Принцип чесності обробки персональних даних.
19. Інші принципи обробки персональних даних (підзвітності і т. п.).
20. Практика Європейського суду з прав людини, щодо застосування принципів обробки персональних даних.

21. Обмеження дії принципів захисту персональних даних.
22. Закріплення принципів захисту персональних даних у джерелах правового регулювання захисту персональних даних.
23. Обмеження дії принципів захисту персональних даних згідно закону.
24. Обмеження дії принципів захисту персональних даних з вимог необхідності та пропорційності.
25. Обмеження дії принципів захисту персональних даних відповідно до легітимних цілей.
26. Права суб'єкта персональних даних та шляхи їх реалізації.
27. Право на доступ до інформації про себе.
28. Право на доступ до інформації про третіх осіб.
29. Право на зміну, модифікацію, видалення персональних даних.
30. Право знати про порядок обробки, адекватний захист персональних даних.
31. Види інформації, яку володілець зобов'язаний надавати суб'єкту персональних даних.
32. Види прав суб'єктів персональних даних.
33. Винятки з права суб'єктів персональних даних на отримання відомостей про себе.
34. Зміст поняття «вмотивованість вимоги» щодо статусу персональних даних.
35. Поняття підстав обробки персональних даних.
36. Згода суб'єкта персональних даних як підстава для їх обробки.
37. Обробка персональних даних на підставі закону.
38. Укладення та виконання правочину, як підстава для обробки персональних даних.
39. Статус персональних даних і конфіденційної інформації та їх співвідношення.
40. Ознаки правомірної згоди на обробку персональних даних.
41. Підстави обробки персональних даних відповідно до закону.
42. Досягнення цілей легітимних інтересів як підстава для обробки персональних даних.
43. Підстави обробки чутливих категорій персональних даних.
44. Практика Європейського Суду з прав людини щодо підстав обробки персональних даних.
45. Легітимні цілі обробки медичної інформації.
46. Поняття захисту персональних даних.

47. Порядок захисту персональних даних відповідно до Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого від 08.01.2014 № 1/02–14.
48. Обов'язки володільця щодо захисту персональних даних.
49. Обов'язки володільця щодо захисту персональних даних, щодо яких здійснюється автоматизована обробка.
50. Зміст захисту персональних даних за замовчуванням (privacy by default).
51. Статус осіб та структурних підрозділів, відповідальних за захист персональних даних.
52. Порядок захисту персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних.
53. Повноваження відповідальної особи/структурного підрозділу, відповідального за захист персональних даних.
54. Практика застосування законодавства щодо захисту персональних даних Уповноваженим Верховної Ради з прав людини.
55. Порядок організації володільцем процесу обробки персональних даних.
56. Елементи обробки персональних даних їх володільцем.
57. Порядок обліку операції, які проводяться з персональними даними їх володільцем.
58. Особливості обробки персональних даних володільцем, який є приватним суб'єктом.
59. Порядок повідомлення Уповноваженого Верховної Ради з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних.
60. Зобов'язання володільця здійснювати повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, та зміст такого повідомлення.
61. Адміністративна відповідальність за неподання повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних.
62. Зобов'язання з повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних відповідно до Директиви Ради Європи.
63. Порядок здійснення контролю за додержанням законодавства про захист персональних даних.

64. Положення законодавства України із здійснення контролю за додержанням законодавства про захист персональних даних.
65. Повноваження представника Уповноваженого з питань захисту персональних даних із контролю за додержанням законодавства про захист персональних даних.
66. Порядок проведення Уповноваженим, його представником та іншими визначеними Уповноваженим службовими особами перевірок.
67. Позапланові перевірки Представника Уповноваженого з питань захисту персональних даних із контролю за додержанням законодавства про захист персональних даних.
68. Права та обов'язки уповноваженої посадової особи та посадових осіб суб'єкта перевірки.
69. Правові наслідки проведення перевірки.
70. Адміністративна відповідальність за результатами перевірки.
71. Тенденції розвитку міжнародної та європейської системи захисту персональних даних.
72. Зміст нового Регламенту Ради міністрів ЄС щодо захисту персональних даних.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ:

А. Спеціальна література:

1. Аналіз Закону України про захист персональних даних: DGI/DP/expertiseUKR(2012) / М. Жорж, Г. Саттон. – Страсбург: Рада Європи, 2012. – 63 с.
2. Бобрик В. І. Право власності на персональні дані [Електронний ресурс] / В. І. Бобрик // Вісник Хмельницького інституту регіонального управління та права. – 2002. – № 2. – С. 114–117.
3. Булеца С. Б. Персональні дані пацієнта [Електронний ресурс] / С. Б. Булеца // Науковий вісник Ужгородського національного університету. Сер.: Право. – 2014. – Вип. 25. – С. 56–61.
4. Городиський І. М. Виконання Україною міжнародних зобов'язань із захисту персональних даних / І. М. Городиський // Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / Упор. Пазюк А. В.; Рец. Гріненко О. О., Олійник О. В. – К.: ФОП Клименко, 2014. – С. 89–97.
5. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України [Текст]: автореф. дис. ... канд. юрид. наук: 12.00.03 / О. А. Дмитренко; НДІ приват. права і п-ва Акад. прав. наук України. – К., 2010. – 19 с.
6. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України [Текст]: дис. ... канд. юрид. наук: 12.00.03 / О. А. Дмитренко; НДІ приват. права і підприємництва Акад. прав. наук України. – К., 2010. – 210 арк. – Бібліогр.: арк. 187–210.
7. Інтеграція України в Європейське інформаційне суспільство: виклики та завдання / Упор. Пазюк А. В. ; Рец. Гріненко О. О., Олійник О. В. – К.: ФОП Клименко, 2014. – 221 с.
8. Каретник О. С. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України [Електронний ре-

сурс] / О. С. Каретник // Часопис Київського університету права. – 2013. – № 2. – С. 228–231.
9. Косіцин М. Проблемні питання правового регулювання повноважень Держспецзв'язку України із захисту інформації про персональні дані / М. Косіцин, Е. Плешко // Прав., нормат. та метрол. забезп. системи захисту інформації в Україні. – 2010. – Вип. 2. – С. 10–13.
10. Макушев П. В. Персональні дані як елемент системи інформаційного забезпечення державної виконавчої служби України / П. В. Макушев // Форум права. – 2013. – № 2. – С. 333–339.
11. Макушев П. В. Системи інформаційного забезпечення державної виконавчої служби України та персональні дані як їх складові / П. В. Макушев // Право і суспільство. – 2013. – № 4. – С. 70–76.
12. Оніщенко О. В. Персональні дані працівників: деякі особливості використання / О. В. Оніщенко // Вісник Академії адвокатури України. – 2012. – Число 3. – С. 173–175.
13. Пазюк А. В. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україна / А. В. Пазюк. – К.: МГО «Прайвесі Юкрейн», 2001. – 260 с.
14. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: Автореф. дис... канд. юрид. наук: 12.00.11 / А. В. Пазюк; Київ. нац. ун-т ім. Т. Шевченка. – К., 2004. – 19 с.
15. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / В. М.Брижко, А. І.Радянська, М. Я.Швець. – К.: Тріумф, 2006. – 256 с.
16. Посібник з європейського права у сфері захисту персональних даних. – К.: К.І.С., 2015. – 216 с.
17. Погребна А. Коментар до Закону України «Про захист персональних даних» / А. Погребна // Юридичний журнал. – 2010. – №7. – [Електронний ресурс]. Цит. 02.09.2010 р. Доступно з – http://www.justinian.com.ua/article.php?id=3579
18. Романюк І. Особливості змісту та реалізації права на персональні дані в Україні та зарубіжних країнах / І. Романюк //

Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки. – 2013. – Вип. 2. – С. 102–106.
19. Романюк І. І. Персональні дані особи як об'єкт цивільного обороту / І. І. Романюк // Право і суспільство. – 2014. – № 6.1(2). – С. 58–65.
20. Сопілко І. М. Генезис змісту категорії «персональні дані» / І. М. Сопілко // Юридичний вісник. Повітряне і космічне право. – 2013. – № 4. – С. 62–66.
21. Чанишев Р. І. Інформація про персональні дані працівника та її захист / Р. І. Чанишев // Актуальні проблеми держави і права. – 2010. – Вип. 52. – С. 94–99.
22. Чанишева Г. І. Право на інформацію за трудовим законодавством України: монографія / Г. І. Чанишева, Р. І. Чанишев. – О.: Фенікс, 2012. – 193 с.
23. Щербіна А. О. Персональні дані в системі інформаційного забезпечення органів місцевого самоврядування / А. О. Щербіна, П. В. Макушев // Публічне право. – 2013. – № 3. – С. 39–46.

В. Іноземна спеціальна література:

1. Bennett C. J. Regulating Privacy: Data Protection and Public Policy in Europe and the United State / C. J. Bennett. – Itaca, NY: Cornell University Press, 1992.
2. Brouwer F. de. Protection of Personal Data: a New Belgian Legal Framework / F. De Brouwer // Revue de Droit Des Affaires Internationales, Paris. – 1999. – No. 2. – P. 181–206.
3. Carey P. Data Protection: A Practical Guide to UK and EU Law: 3rd Edt. / P. Carey. – Oxford University Press, Inc. New York, NY, USA: 2009.
   Dumortier J. The Protection of Personal Data in the Schengen Convention / J. Dumortier // International Review of Law Computers and Technology, Cambridge. – 1997. – March. – Vol. 11. – No. 1. – P. 93–106.
4. Fleischmann A. Personal Data Security: Divergent Standards in the European Union and the United States / A. Fleischmann // Fordham International Law Journal, New York. – 1995. – October. – Vol. 19. – No. 1. – P. 143–180.

5. Heisenberg D. Negotiating Privacy: The European Union, the United States, and Personal Data Protection / D. Heisenberg. – Boulder, CO, USA: Lynne Rienner Publisers, 2005.
6. Platten N. Orchestrating Transatlantic Approaches to Personal Data Protection: a European Perspective / N. Platten // Fordham International Law Journal, New York. – 1999. – June. – Vol. 22. – No. 5. – P. 2024–2051.
7. Pearce G. Achieving Personal Data Protection in the European Union / G. Pearce, N. Platten // Journal of Common Market Studies, Oxford. – 1998. – Vol. 36. –No. 4. – P. 529–547.
8. Simitis S. Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data / S. Spiros // European Law Journal, Oxford. – 1999. – March. – Vol. 5. – No. 1. – P. 45–62.
9. Warren S. Rights to Privacy / S. Warre, L. Brandeis // Harvard Law Review. – 1890. – Vol. 4. – No. 5. – P. 193–220.

С. Міжнародно-правові акти:

1. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) as amended on 11 July 2013 by C(2013)79 / OECD. – [Electronic source]. Cit. 02.09.2014. Retrieved from – http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.
2. Резолюция Генеральной Ассамблеи ООН №95 (XLV) от 14 декабря 1946 г. : A/45/PV.68 / Организация Объединенных Наций. – Официальный сайт ООН. – [Электронный ресурс]. Цит. 02.09.2014 г. Режим доступа – http://www.un.org/ru/documents/ods.asp?m=A/RES/45/95.
3. 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.
4. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 р. / Рада Європи. – Офіційний вісник України

від 14.01.2011 р. – Офіц. Вид. – 2010/2011. – № 58 / № 58, 2010, ст. 1994 / стор. 708, стаття 86, код акту 54294/2011.
5. 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. 02.09.2014 р. Режим доступу – http://zakon4.rada.gov.ua/laws/show/994_242.

D. Національне законодавство:

1. 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.
2. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних: Закон України №3454-VI від 2 червня 2011 р. / Верховна Рада України. – Офіційний вісник України офіційне видання від 04.07.2011 р. – 2011. – № 48. – Стор. 42, стаття 1954, код акту 57277/2011.
3. Про затвердження документів у сфері захисту персональних даних: Наказ № 1/02–14 від 08.01.2014 р. / Уповноважений Верховної Ради України із прав людини. – Баланс від 06.03.2014 р. – 2014. – № 19. – Стор. 5.
4. Про Єдиний державний демографічний реєстр: Закон України № 5492-VI від 20.11.2012 р. / Верховна Рада України. – Офіційний вісник України від 14.12.2012 р. – Офіц. вид. – 2012. – № 93. – Стор. 122, стаття 3771, код акту 64640/2012.

E. Законодавство зарубіжних країн:

1. Великобританія: Data Protection Act 1998 // [Electronic source] – Cit. 24.05.2015. – Retrieved from – http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf.
2. Ірландія: Data Protection Act, 1988 // [Electronic source] – Cit. 24.05.2015. – Retrieved from – http://www.irishstatutebook.ie/1988/en/act/pub/0025/print.html.

3. Італія: Data Protection Code – Legislative Decree no. 196/2003 // [Electronic source] – Cit. 24.05.2015. – Retrieved from – http://www.privacy.it/privacycode-en.html.
4. Німеччина: Federal Data Protection Act in the version promulgated on 14 January 2003 // [Electronic source] – Cit. 24.05.2015. – Retrieved from – http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf.
5. Польща: The Act of 29 August 1997 on the Protection of Personal Data (unified text: Journal of Laws of 2014, item 1182 with amendments) // [Electronic source] – Cit. 24.05.2015. – Retrieved from – http://www.giodo.gov.pl/144/id_art/171/j/en/.
6. Чехія: Act No. 101/2000 Coll., of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts // [Electronic source] – Cit. 24.05.2015. – Retrieved from – https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1107.
7. Чорногорія: Personal Data Protection Law // [Electronic source] – Cit. 24.05.2015. – Retrieved from – http://www.afapdp.org/wp-content/uploads/2012/01/Mont%C3%A9n%C3%A9gro-Personal-Data-Protection-Law-79–08-and-70–09.pdf.

ДОДАТКИ

ЗАКОН УКРАЇНИ

Про захист персональних даних

(Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)

{Із змінами, внесеними згідно із Законами
№ 4452-VI від 23.02.2012, ВВР, 2012, № 50, ст.564
№ 5491-VI від 20.11.2012, ВВР, 2013, № 51, ст.715
№ 245-VII від 16.05.2013, ВВР, 2014, № 12, ст.178
№ 383-VII від 03.07.2013, ВВР, 2014, № 14, ст.252
№ 1170-VII від 27.03.2014, ВВР, 2014, № 22, ст.816
№ 1262-VII від 13.05.2014, ВВР, 2014, № 27, ст.914
№ 316-VIII від 09.04.2015}

{У тексті Закону слова «володілець бази персональних даних» і «розпорядник бази персональних даних» у всіх відмінках і числах замінено відповідно словами «володілець персональних даних» і «розпорядник персональних даних» у відповідному відмінку і числі згідно із Законом № 5491-VI від 20.11.2012}

Стаття 1. Сфера дії Закону

Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що

містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

{Частину третю статті 1 виключено на підставі Закону № 383-VII від 03.07.2013}

{Частину четверту статті 1 виключено на підставі Закону № 383-VII від 03.07.2013}

{Стаття 1 в редакції Закону № 5491-VI від 20.11.2012}

Стаття 2. Визначення термінів

У цьому Законі нижченаведені терміни вживаються в такому значенні:

база персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

{Абзац третій статті 2 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 383-VII від 03.07.2013}

згода суб'єкта персональних даних – 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;

{Абзац четвертий статті 2 в редакції Закону № 1262-VII від 13.05.2014}

{Абзац п'ятий статті 2 виключено на підставі Закону № 383-VII від 03.07.2013}

знеособлення персональних даних – вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

{Абзац шостий статті 2 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

картотека – будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами;

{Статтю 2 доповнено терміном згідно із Законом № 5491-VI від 20.11.2012}

обробка персональних даних – 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;

{Абзац статті 2 в редакції Закону № 5491-VI від 20.11.2012}

одержувач – фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа;

{Статтю 2 доповнено терміном згідно із Законом № 5491-VI від 20.11.2012}

персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

розпорядник персональних даних – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця;

{Абзац одинадцятий статті 2 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

суб'єкт персональних даних – фізична особа, персональні дані якої обробляються;

{Абзац дванадцятий статті 2 в редакції Закону № 383-VII від 03.07.2013}

третя особа – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

{Абзац тринадцятий статті 2 в редакції Закону № 383-VII від 03.07.2013}

Стаття 3. Законодавство про захист персональних даних

Законодавство про захист персональних даних складають Конституція України, цей Закон, інші закони та підзаконні нормативно-правові акти, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України.

Стаття 4. Суб'єкти відносин, пов'язаних із персональними даними

1. Суб'єктами відносин, пов'язаних із персональними даними, є:

суб'єкт персональних даних;

володілець персональних даних;

розпорядник персональних даних;

третя особа;

Уповноважений Верховної Ради України з прав людини (далі – Уповноважений).

{Абзац шостий частини першої статті 4 в редакції Закону № 383-VII від 03.07.2013}

{Абзац сьомий частини першої статті 4 виключено на підставі Закону № 5491-VI від 20.11.2012}

2. Володільцем чи розпорядником персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону.

3. 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.

{Частина третя статті 4 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

4. Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі.

{Статтю 4 доповнено частиною четвертою згідно із Законом № 5491-VI від 20.11.2012}

5. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.

{Статтю 4 доповнено частиною п'ятою згідно із Законом № 5491-VI від 20.11.2012}

Стаття 5. Об'єкти захисту

1. Об'єктами захисту є персональні дані.

2. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень.

3. Персональні дані, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, оформленій за формою і в порядку, встановленими Законом України «Про засади запобігання і протидії корупції», не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України «Про засади запобігання і протидії корупції».

Не належить до інформації з обмеженим доступом інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених статтею 6 Закону України «Про доступ до публічної інформації».

Законом може бути заборонено віднесення інших відомостей, що є персональними даними, до інформації з обмеженим доступом.

{Стаття 5 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 1170-VII від 27.03.2014}

Стаття 6. Загальні вимоги до обробки персональних даних

1. 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.

Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

{Частину першу статті 6 доповнено новим абзацом згідно із Законом № 5491-VI від 20.11.2012}

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.

{Абзац третій частини першої статті 6 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 383-VII від 03.07.2013}

2. Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки.

{Частина друга статті 6 в редакції Закону № 5491-VI від 20.11.2012}

3. Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки.

{Абзац перший частини третьої статті 6 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

{Абзац другий частини третьої статті 6 виключено на підставі Закону № 5491-VI від 20.11.2012}

4. Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

5. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

6. Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

{Частина шоста статті 6 із змінами, внесеними згідно із Законом № 1170-VII від 27.03.2014}

7. Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

8. Персональні дані обробляються 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.

Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту.

{Частина восьма статті 6 в редакції Закону № 383-VII від 03.07.2013}

{Частину дев'яту статті 6 виключено на підставі Закону № 383-VII від 03.07.2013}

10.Типовий порядок обробки персональних даних затверджується Уповноваженим.

{Частина десята статті 6 із змінами, внесеними згідно із Законами № 4452-VI від 23.02.2012,№ 5491-VI від 20.11.2012; в редакції Законів № 383-VII від 03.07.2013, № 1262-VII від 13.05.2014}

Стаття 7. Особливі вимоги до обробки персональних даних

1. Забороняється обробка 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.

{Частина перша статті 7 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 383-VII від 03.07.2013}

2. Положення частини першої цієї статті не застосовується, якщо обробка персональних даних:

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

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

{Пункт 2 частини другої статті 7 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012*}*

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;

{Пункт 3 частини другої статті 7 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

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;

{Пункт 4 частини другої статті 7 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

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

6) необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я, на якого покладено обов'язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю;

{Пункт 6 частини другої статті 7 в редакції Закону № 5491-VI від 20.11.2012}

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

{Пункт 7 частини другої статті 7 із змінами, внесеними згідно із Законом № 245-VII від 16.05.2013; в редакції Закону № 383-VII від 03.07.2013}

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

{Пункт 8 частини другої статті 7 із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

Стаття 8. Права суб'єкта персональних даних

1. Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

2. 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;

{Пункт 1 частини другої статті 8 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 383-VII від 03.07.2013}

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

{Пункт 2 частини другої статті 8 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

3) на доступ до своїх персональних даних;

{Пункт 3 частини другої статті 8 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

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;

{Пункт 4 частини другої статті 8 в редакції Закону № 383-VII від 03.07.2013}

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

{Пункт 5 частини другої статті 8 в редакції Закону № 5491-VI від 20.11.2012}

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;

{Пункт 6 частини другої статті 8 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

7) на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

8) звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

{Пункт 8 частини другої статті 8 в редакції Закону № 5491-VI від 20.11.2012; із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

{Частину другу статті 8 доповнено пунктом 10 згідно із Законом № 5491-VI від 20.11.2012}

11) відкликати згоду на обробку персональних даних;

{Частину другу статті 8 доповнено пунктом 11 згідно із Законом № 5491-VI від 20.11.2012}

12) знати механізм автоматичної обробки персональних даних;

{Частину другу статті 8 доповнено пунктом 12 згідно із Законом № 5491-VI від 20.11.2012}

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

{Частину другу статті 8 доповнено пунктом 13 згідно із Законом № 5491-VI від 20.11.2012}

{Частину третю статті 8 виключено на підставі Закону № 383-VII від 03.07.2013}

Стаття 9. Повідомлення про обробку персональних даних

1. 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, визначаються Уповноваженим.

2. Повідомлення про обробку персональних даних подається за формою та в порядку, визначеними Уповноваженим.

3. Володілець персональних даних зобов'язаний повідомляти Уповноваженого про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни.

4. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого в порядку, визначеному Уповноваженим.

{Стаття 9 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 383-VII від 03.07.2013}

Стаття 10. Використання персональних даних

1. Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.

{Частина перша статті 10 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

2. Використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володіль-

цю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

{Частина друга статті 10 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

3. Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники 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, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

{Частина третя статті 10 із змінами, внесеними згідно із Законом № 1170-VII від 27.03.2014}

4. Відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості.

Стаття 11. Підстави для обробки персональних даних

1. Підставами для обробки персональних даних є:

1) згода суб'єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

3) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом;

{Частину першу статті 11 доповнено новим пунктом згідно із Законом № 383-VII від 03.07.2013}

6) необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб'єкт персональ-

них даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес.

{Пункт 6 частини першої статті 11 в редакції Закону № 383-VII від 03.07.2013}

{Стаття 11 в редакції Закону № 5491-VI від 20.11.2012}

Стаття 12. Збирання персональних даних

1. Збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

{Частина перша статті 12 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

2. Суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані:

в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;

в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

{Частина друга статті 12 в редакції Законів № 5491-VI від 20.11.2012, № 383-VII від 03.07.2013}

{Частину третю статті 12 виключено на підставі Закону № 5491-VI від 20.11.2012}

{Частину четверту статті 12 виключено на підставі Закону № 5491-VI від 20.11.2012}

Стаття 13. Накопичення та зберігання персональних даних

1. Накопичення персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних.

2. Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.

Стаття 14. Поширення персональних даних

1. Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних.

{Частина перша статті 14 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

2. Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

{Частина друга статті 14 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

3. Виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані.

4. Сторона, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог цього Закону.

Стаття 15. Видалення або знищення персональних даних

{Назва статті 15 в редакції Закону № 5491-VI від 20.11.2012}

1. Персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону.

{Частина перша статті 15 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

2. Персональні дані підлягають видаленню або знищенню у разі:

{Абзац перший частини другої статті 15 із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;

2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;

3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;

{Підпункт 3 частини другої статті 15 в редакції Закону № 383-VII від 03.07.2013}

4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

{Частину другу статті 15 доповнено підпунктом 4 згідно із Законом № 383-VII від 03.07.2013*}*

3. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

{Частина третя статті 15 із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

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

{Частина четверта статті 15 із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

{Текст статті 15 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

Стаття 16. Порядок доступу до персональних даних

1. Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю персональних даних на обробку цих даних, або відповідно до вимог закону. Порядок доступу третіх осіб до персональних даних, які знаходяться у володінні розпорядника публічної інформації, визначається Законом України «Про доступ до публічної інформації».

{Частина перша статті 16 із змінами, внесеними згідно із Законом № 1170-VII від 27.03.2014}

2. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити.

3. Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу (далі – запит) до персональних даних володільцю персональних даних.

4. 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;

{Пункт 4 частини четвертої статті 16 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

5) перелік персональних даних, що запитуються;

6) мета та/або правові підстави для запиту.

{Пункт 6 частини четвертої статті 16 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

5. Строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження.

Протягом цього строку володілець персональних даних доводить до відома особи, яка подає запит, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

6. Суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання інформації, визначеної у пункті 1 частини четвертої цієї статті, крім випадків, установлених законом.

{Частина шоста статті 16 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

Стаття 17. Відстрочення або відмова у доступі до персональних даних

1. Відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.

2. Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.

Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

У повідомленні про відстрочення зазначаються:

1) прізвище, ім'я та по батькові посадової особи;

2) дата відправлення повідомлення;

3) причина відстрочення;

4) строк, протягом якого буде задоволено запит.

3. Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із законом.

У повідомленні про відмову зазначаються:

1) прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;

2) дата відправлення повідомлення;

3) причина відмови.

Стаття 18. Оскарження рішення про відстрочення або відмову в доступі до персональних даних

1. Рішення про відстрочення або відмову у доступі до персональних даних може бути оскаржено до Уповноваженого Верховної Ради України з прав людини або суду.

{Частина перша статті 18 в редакції Закону № 5491-VI від 20.11.2012; із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

2. Якщо запит зроблено суб'єктом персональних даних щодо даних про себе, обов'язок доведення в суді законності відмови у доступі покладається на володільця персональних даних, до якого подано запит.

{Частина друга статті 18 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012}

Стаття 19. Оплата доступу до персональних даних

1. Доступ суб'єкта персональних даних до даних про себе здійснюється безоплатно.

2. Доступ інших суб'єктів відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи чи групи фізичних осіб може бути платним у разі додержання умов, визначених цим Законом. Оплаті підлягає робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних.

3. Розмір плати за послуги з надання доступу до персональних даних органами державної влади визначається Кабінетом Міністрів України.

4. Органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їх повноважень.

Стаття 20. Зміни і доповнення до персональних даних

1. Володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних.

{Частина перша статті 20 із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

2. Володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних також за зверненням інших суб'єктів відносин, пов'язаних із персональними даними, якщо на це є згода суб'єкта персональних даних чи відповідна зміна здійснюється згідно з приписом Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого чи за рішенням суду, що набрало законної сили.

{Частина друга статті 20 в редакції Закону № 383-VII від 03.07.2013}

3. Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності.

Стаття 21. Повідомлення про дії з персональними даними

1. Про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом.

2. Повідомлення, зазначені у частині першій цієї статті, не здійснюються 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 12цього Закону.

{Частину другу статті 21 доповнено пунктом 4 згідно із Законом № 5491-VI від 20.11.2012}

3. 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.

{Частина третя статті 21 із змінами, внесеними згідно із Законом № 383-VII від 03.07.2013}

Стаття 22. Контроль за додержанням законодавства про захист персональних даних

1. Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи:

1) Уповноважений;

2) суди.

{Стаття 22 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; текст статті 22 в редакції Закону № 383-VII від 03.07.2013}

Стаття 23. Повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних

1. Уповноважений має такі повноваження у сфері захисту персональних даних:

1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;

2) проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

3) отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;

4) затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом;

5) за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

6) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і

обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

7) взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб;

8) звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

9) надавати за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них;

10) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

11) інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними;

12) здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних;

13) організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних;

14) брати участь у роботі міжнародних організацій з питань захисту персональних даних.

2. Уповноважений Верховної Ради України з прав людини включає до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних.

{Стаття 23 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 383-VII від 03.07.2013}

Стаття 24. Забезпечення захисту персональних даних

1. 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.

2. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

3. Структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із 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.

4. Фізичні особи – підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону.

{Стаття 24 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012; в редакції Закону № 383-VII від 03.07.2013}

Стаття 25. Обмеження дії цього Закону

1. 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.

2. Дозволяється обробка персональних даних без застосування положень цього Закону, якщо така обробка здійснюється:

1) фізичною особою виключно для особистих чи побутових потреб;

2) виключно для журналістських та творчих цілей, за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів.

3. Дія цього Закону не поширюється на відносини щодо отримання архівної інформації репресивних органів.

{Статтю 25 доповнено частиною третьою згідно із Законом № 316-VIII від 09.04.2015}

{Стаття 25 в редакції Закону № 383-VII від 03.07.2013}

Стаття 26. Фінансування робіт із захисту персональних даних

Фінансування робіт та заходів щодо забезпечення захисту персональних даних здійснюється за рахунок коштів Державного бюджету України та місцевих бюджетів, коштів суб'єктів відносин, пов'язаних із персональними даними.

Стаття 27. Застосування положень цього Закону

1. Положення щодо захисту персональних даних, викладені в цьому Законі, можуть доповнюватися чи уточнюватися іншими законами, за умови, що вони встановлюють вимоги щодо захисту персональних даних, що не суперечать вимогам цього Закону.

2. Професійні, самоврядні та інші громадські об'єднання чи юридичні особи можуть розробляти кодекси поведінки з метою забезпечення ефективного захисту прав суб'єктів персональних даних, додержання законодавства про захист персональних даних з урахуванням специфіки обробки персональних даних у різних сферах. При розробленні такого кодексу поведінки або внесенні змін до нього відповідне об'єднання чи юридична особа може звернутися за висновком до Уповноваженого.

{Частина друга статті 27 із змінами, внесеними згідно із Законом № 5491-VI від 20.11.2012*; в редакції Закону № 383-VII від 03.07.2013}*

Стаття 28. Відповідальність за порушення законодавства про захист персональних даних

Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом.

Стаття 29. Міжнародне співробітництво та передача персональних даних

{Назва статті 29 в редакції Закону № 5491-VI від 20.11.2012}

1. Співробітництво з іноземними суб'єктами відносин, пов'язаних із персональними даними, регулюється Конституцією України, цим Законом, іншими нормативно-правовими актами та міжнародними договорами України.

2. Якщо міжнародним договором України, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені законодавством України, то застосовуються правила міжнародного договору України.

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

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

Кабінет Міністрів України визначає перелік держав, які забезпечують належний захист персональних даних.

Персональні дані не можуть поширюватися з іншою метою, ніж та, з якою вони були зібрані.

{Частина третя статті 29 в редакції Закону № 5491-VI від 20.11.2012}

4. Персональні дані можуть передаватися іноземним суб'єктам відносин, пов'язаних з персональними даними, також у разі:

1) надання суб'єктом персональних даних однозначної згоди на таку передачу;

2) необхідності укладення чи виконання правочину між володільцем персональних даних та третьою особою – суб'єктом персональних даних на користь суб'єкта персональних даних;

3) необхідності захисту життєво важливих інтересів суб'єктів персональних даних;

4) необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги;

5) надання володільцем персональних даних відповідних гарантій щодо невтручання в особисте і сімейне життя суб'єкта персональних даних.

{Статтю 29 доповнено частиною четвертою згідно із Законом № 5491-VI від 20.11.2012}

Стаття 30. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2011 року.

2. Кабінету Міністрів України протягом шести місяців з дня набрання чинності цим Законом:

забезпечити прийняття нормативно-правових актів, передбачених цим Законом;

забезпечити приведення своїх нормативно-правових актів у відповідність із цим Законом.

Президент України В. ЯНУКОВИЧ
м. Київ
1 червня 2010 року
№ 2297-VI

Публікації документа

- **Урядовий кур'єр** від 07.07.2010 – № 122
- **Офіційний вісник України** від 09.07.2010–2010 р., № 49, стор. 199, стаття 1604, код акту 51762/2010
- **Відомості Верховної Ради України** від 27.08.2010–2010 р., № 34, стор. 1188, стаття 481
- **Голос України** від 16.09.2010 – № 172

Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних

Страсбург, 28 січня 1981 року

Статус Конвенції див. (994_542**)**

*{Додатковий протокол див. в документі (*994_363*) від 08.11.2001}*

*{Конвенцію ратифіковано із заявами згідно із Законом N 2438-VI (*2438–17*) від 06.07.2010}*

Дата підписання: 28.01.1981
Дата ратифікації Україною: 06.07.2010
Дата набрання чинності для України: 01.01.2011

Офіційний переклад

Преамбула

Держави-члени Ради Європи, які підписали цю Конвенцію,

беручи до уваги те, що метою Ради Європи є досягнення більшого єднання між її членами, яке ґрунтується, зокрема, на дотриманні верховенства права, а також прав людини й основоположних свобод;

беручи до уваги те, що бажано поширювати гарантії прав й основоположних свобод кожної людини, зокрема права на повагу до недоторканості приватного життя, з огляду на зростання транскордонного потоку персональних даних, які піддаються автоматизованій обробці;

підтверджуючи водночас свою відданість свободі інформації незалежно від кордонів;

визнаючи необхідність узгодження основоположних цінностей поваги до недоторканості приватного життя й безперешкодного обміну інформацією між народами;

домовилися про таке:

Глава I
Загальні положення

Стаття 1
Предмет і мета

Метою цієї Конвенції є забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав й основоположних свобод, зокрема її права на недоторканість приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються (далі – захист даних).

Стаття 2
Визначення

Для цілей цієї Конвенції:

a) термін «персональні дані» означає будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (далі – суб'єкт даних);

b) термін «файл даних для автоматизованої обробки» означає будь-який масив даних, що піддається автоматизованій обробці;

c) термін «автоматизована обробка» включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних та (або) арифметичних операцій із цими даними, їхню зміну, знищення, вибірку або поширення;

d) термін «контролер файлу» означає фізичну або юридичну особу, державний орган, установу чи будь-який інший орган, що уповноважений відповідно до національного законодавства вирішувати, яким повинно бути призначення файлу даних для автоматизованої обробки, які категорії персональних даних повинні зберігатися та які операції повинні здійснюватися з ними.

Стаття 3
Сфера застосування

1. Сторони зобов'язуються застосовувати цю Конвенцію до файлів персональних даних для автоматизованої обробки та до автоматизованої обробки персональних даних у державному та приватному секторах.

2. Будь-яка Держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або документа про прийняття, схвалення або приєднання чи будь-коли в подальшому може повідомити за допомогою заяви на ім'я Генерального секретаря Ради Європи про те, що вона:

a) не буде застосовувати цієї Конвенції до певних категорій файлів персональних даних для автоматизованої обробки, перелік яких буде зданий на зберігання. Однак до цього переліку вона не повинна включати категорії файлів даних для автоматизованої обробки, які згідно з її внутрішнім законодавством підпадають під дію положень про захист даних. Отже, вона не повинна вносити змін до цього переліку за допомогою нової заяви щоразу, коли згідно з її внутрішнім законодавством під дію положень про захист персональних даних підпадають додаткові категорії файлів персональних даних для автоматизованої обробки;

b) також буде застосовувати цю Конвенцію до інформації, яка стосується груп осіб, асоціацій, фондів, компаній, корпорацій та будь-яких інших організацій, що безпосередньо чи опосередковано складаються з окремих осіб, незалежно від того, мають чи не мають такі установи статус юридичної особи;

c) також буде застосовувати цю Конвенцію до файлів персональних даних, які не обробляються автоматизовано.

3. Будь-яка Держава, що поширила сферу застосування цієї Конвенції за допомогою будь-якої із заяв, передбачених у підпунктах «b» і «c» викладеного вище пункту 2, може повідомити в зазначеній заяві, що такі поширення сфери застосування цієї Конвенції стосується лише певних категорій файлів персональних даних, перелік яких буде зданий на зберігання.

4. Будь-яка Сторона, яка за допомогою заяви, передбаченої в підпункті «a» викладеного вище пункту 2, виключила певні категорії файлів персональних даних для автоматизованої обробки, не може вимагати застосування Конвенції до таких категорій Стороною, яка не виключила їх.

5. Так само Сторона, яка не здійснила того чи того поширення, передбаченого в підпунктах «b» і «c» викладеного вище пункту 2, не може вимагати застосування цієї Конвенції за цими підпунктами стосовно Сторони, яка здійснила такі поширення.

6. Заяви, передбачені у викладеному вище пункті 2, набувають чинності з моменту набуття чинності Конвенцією для Держави, яка їх зробила, якщо такі заяви було зроблено під час підписання або здачі на зберігання її ратифікаційної грамоти або документа про прийняття, схвалення чи приєднання або через три місяці після отримання їх Генеральним секретарем Ради Європи, якщо вони їх було зроблено будь-коли в подальшому. Такі заяви можуть бути відкликані повністю або частково за допомогою повідомлення на ім'я Генерального секретаря Ради Європи. Такі відкликання набувають чинності через три місяці з дати тримання такого повідомлення.

Глава II
Основні принципи захисту даних

Стаття 4
Обов'язки Сторін

1. Кожна Сторона вживає необхідних заходів стосовно свого внутрішнього законодавства для набуття чинності основними принципами захисту даних, викладеними в цій главі.

2. Таких заходів уживають принаймні тоді, коли ця Конвенція набуває чинності для відповідної Сторони.

Стаття 5
Якість даних

Персональні дані, що піддаються автоматизованій обробці, повинні:

a) отримуватися та оброблятися сумлінно та законно;

b) зберігатися для визначених і законних цілей та не використовуватися в спосіб, не сумісний із цими цілями;

c) бути адекватними, відповідними та ненадмірними стосовно цілей, для яких вони зберігаються;

d) бути точними та в разі необхідності оновлюватися;

e) зберігатись у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються.

Стаття 6
Особливі категорії даних

Персональні дані, що свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Це правило також застосовується до персональних даних, що стосуються засудження в кримінальному порядку.

Стаття 7
Безпека даних

Для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, уживають відповідних заходів безпеки, спрямованих на запобігання випадковому чи несанкціонованому знищенню або випадковій утраті, а також на запобігання несанкціонованим доступу, зміні або поширенню.

Стаття 8
Додаткові гарантії для суб'єкта даних

Будь-якій особі надається можливість:

a) з'ясувати існування файлу персональних даних для автоматизованої обробки, його головні цілі, а також особу та постійне місце проживання чи головне місце роботи контролера файлу;

b) отримувати через обґрунтовані періоди та без надмірної затримки або витрат підтвердження або спростування факту зберігання персональних даних, що її стосуються, у файлі даних для автоматизованої обробки, а також отримувати такі дані в доступній для розуміння формі;

c) вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися всупереч положенням внутрішнього законодавства, що запроваджують основоположні принципи, визначені у статтях 5 і 6 цієї Конвенції;

d) використовувати засоби правового захисту в разі невиконання передбаченого в пунктах «b» і «c» цієї статті прохання про підтвердження або у відповідних випадках про надання, виправлення або знищення персональних даних.

Стаття 9

Винятки та обмеження

1. Винятки з положень статей 5, 6 та 8 цієї Конвенції дозволяються лише в рамках, визначених цією статтею.

2. Відхилення від положень статей 5, 6 та 8 цієї Конвенції дозволяється тоді, коли таке відхилення передбачене законодавством Сторони та є в демократичному суспільстві необхідним заходом, спрямованим на:

a) захист державної та громадської безпеки, фінансових інтересів Держави або на боротьбу з кримінальними правопорушеннями;

b) захист суб'єкта даних або прав і свобод інших людей.

3. Обмеження стосовно здійснення прав, визначених у пунктах «b», «c» та «d» статті 8, можуть установлюватися законодавством стосовно файлів персональних даних для автоматизованої обробки, що використовуються для цілей статистики або наукових досліджень у випадках явної відсутності небезпеки порушення недоторканості приватного життя суб'єктів даних.

Стаття 10

Санкції та засоби правового захисту

Кожна Сторона зобов'язується встановити відповідні санкції та засоби правового захисту стосовно порушень положень внутрішнього права, що запроваджують основоположні принципи захисту персональних даних, визначені в цій главі.

Стаття 11

Розширення захисту

Жодне з положень цієї глави не тлумачиться як таке, що обмежує можливості Сторони забезпечувати суб'єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією, або як таке, що іншим чином завдає шкоди такій можливості.

Глава III
Транскордонні потоки даних

Стаття 12
Транскордонні потоки персональних даних та внутрішнє законодавство

1. Стосовно передачі через національні кордони за допомогою будь-яких засобів персональних даних, що піддаються автоматизованій обробці або зібраних з метою їхньої автоматизованої обробки, застосовуються такі положення.

2. Сторона не може лише з метою захисту недоторканості приватного життя забороняти чи обумовлювати спеціальними дозволами транскордонні потоки персональних даних, що передаються на територію іншої Сторони.

3. Однак кожна Сторона має право відступати від положень пункту 2:

a) якщо її законодавство містить конкретні положення для певних категорій персональних даних або файлів персональних даних для автоматизованої обробки, у зв'язку з особливостями цих даних або файлів, за винятком випадків, коли положення іншої Сторони забезпечують аналогічний захист;

b) якщо передача даних здійснюється з її території на територію Держави, що не є Договірною Державою, через територію іншої Сторони, для запобігання порушенню такою передачею законодавства Сторони, зазначеної на початку цього пункту.

Глава IV
Взаємна допомога

Стаття 13
Співробітництво між Сторонами

1. Сторони погоджуються надавати одна одній взаємну допомогу для реалізації цієї Конвенції.

2. Для цього:

a) кожна Сторона призначає один чи більше органів, назву та адресу яких вона повідомляє Генеральному секретарю Ради Європи;

b) кожна Сторона, яка призначила більше одного органу, зазначає у своєму повідомленні, згаданому в попередньому підпункті, сферу повноважень кожного з них.

3. Орган, призначений однією Стороною, на прохання органу, призначеного іншою Стороною:

a) надає інформацію про своє законодавство та адміністративну практику в галузі захисту даних;

b) відповідно до свого внутрішнього законодавства та виключно з метою захисту недоторканості приватного життя вживає всіх відповідних заходів для надання фактичної інформації стосовно конкретної автоматизованої обробки, яка здійснюється на його території, але за винятком персональних даних, що обробляються.

Стаття 14

Допомога суб'єктам даних, які проживають за кордоном

1. Кожна Сторона надає допомогу будь-якій особі, яка постійно проживає за кордоном, у здійсненні прав, наданих її внутрішнім законодавством, що запроваджує принципи, визначені в статті 8 цієї Конвенції.

2. Якщо така особа проживає на території іншої Сторони, їй надається можливість подати своє прохання за посередництвом органу, призначеного цією Стороною.

3. Прохання про надання допомоги повинно містити всі необхідні відомості, що стосуються, inter alia:

a) прізвища, адреси та будь-яких інших відповідних відомостей, які встановлюють особу, що звертається з проханням;

b) файлу персональних даних для автоматизованої обробки, якого стосується прохання, або його контролера;

c) мети прохання.

Стаття 15

Гарантії стосовно допомоги, що надається призначеними органами

1. Орган, який призначений однією Стороною і який отримав від органу, призначеного іншою Стороною, інформацію, що супроводжує прохання про надання допомоги, або інформацію у відповідь на його прохання про надання допомоги, використовує цю інформацію лише для цілей, зазначених у проханні про надання допомоги.

2. Кожна Сторона забезпечує, щоб особи, які працюють у призначеному органі або діють від його імені, мали відповідні зобов'язання стосовно збереження таємності або конфіденційності такої інформації.

3. Призначеному органу на свій розсуд і без ясно вираженої згоди суб'єкта даних, що проживає за кордоном, у жодному випадку не дозволяється звертатися згідно з пунктом 2 статті 14 з проханням про надання допомоги від імені відповідної особи.

Стаття 16

Відхилення прохань про надання допомоги

Призначений орган, до якого надіслано прохання про надання допомоги згідно зі статтями 13 або 14 цієї Конвенції, може відмовитися задовольняти таке прохання, якщо:

a) прохання є не сумісним з повноваженнями, якими наділені в галузі захисту персональних даних органи, що відповідають за виконання прохання;

b) прохання не відповідає положенням цієї Конвенції;

виконання прохання порушило б суверенітет, безпеку або громадський порядок (ordre public) Сторони, якою він був призначений, або права та основоположні свободи осіб, які знаходяться під юрисдикцією цієї Сторони.

Стаття 17

Витрати на допомогу та порядок її надання

1. Взаємна допомога, яку Сторони надають одна одній згідно зі статтею 13, та допомога, яку вони надають згідно зі статтею 14 суб'єктам даних, що проживають за кордоном, не може бути підставою для сплати жодних витрат або зборів, за винятком тих, що сплачуються у зв'язку з діяльністю експертів і перекладачів.

Витрати або збори у зв'язку з діяльністю останніх сплачуються Стороною, яка призначила орган, що звертається з проханням про надання допомоги.

2. На суб'єкта даних не може покладатися сплата витрат або зборів, пов'язаних із заходами, яких було вжито від його імені на території іншої Сторони, крім витрат або зборів, які на законних підставах сплачуються резидентами такої Сторони.

3. Інші подробиці стосовно надання допомоги, що стосуються, зокрема, форм і процедур, а також використання мов, визначаються безпосередньо між відповідними Сторонами.

Глава V
Консультативний комітет

Стаття 18
Склад Комітету

1. Консультативний комітет створюється після набуття чинності цією Конвенцією.

2. Кожна Сторона призначає до Комітету одного представника та заступника представника. Будь-яка Держава – член Ради Європи, яка не є Стороною Конвенції, має право бути представленою в Комітеті спостерігачем.

Консультативний комітет одностайним рішенням може запропонувати будь-якій Державі, яка не є членом Ради Європи і не є Стороною Конвенції, бути представленою на тому чи тому засіданні як спостерігач.

Стаття 19
Функції Комітету

Консультативний комітет:

a) може вносити пропозиції для сприяння застосуванню або поліпшення застосування Конвенції;

b) може вносити пропозиції стосовно внесення змін та доповнень до цієї Конвенції відповідно до статті 21;

c) надає свій висновок стосовно будь-якої пропозиції про внесення змін та доповнень до цієї Конвенції, які передаються йому на розгляд відповідно до пункту 3 статті 21;

d) на прохання Сторони може робити висновок з будь-якого питання, що стосується застосування цієї Конвенції.

Стаття 20
Процедура

1. Консультативний комітет скликається Генеральним секретарем Ради Європи. Його перше засідання відбувається у рамках дванадцяти місяців після набрання чинності цією Конвенцією. У по-

дальшому він збирається принаймні раз на два роки й у будь-якому разі, коли одна третина представників Сторін вимагає його скликання.

2. Кворумом засідання Консультативного комітету є більшість представників Сторін.

3. Після кожного свого засідання Консультативний комітет подає Комітетові Міністрів Ради Європи звіт про свою роботу та про стан виконання Конвенції.

4. Відповідно до положень цієї Конвенції Консультативний комітет складає свій регламент.

Глава VI
Зміни

Стаття 21
Зміни

1. Зміни до цієї Конвенції можуть пропонуватися Стороною, Комітетом Міністрів Ради Європи або Консультативним комітетом.

2. Будь-яка пропозиція про внесення зміни надсилається Генеральним секретарем Ради Європи Державам-членам Ради Європи та кожній Державі, що не є членом Ради Європи, яка приєдналася до цієї Конвенції або якій було запропоновано приєднатися до неї відповідно до положень статті 23.

3. Крім того, будь-яку зміну, запропоновану Стороною або Комітетом Міністрів, надсилають Консультативному комітетові, який подає Комітетові міністрів свої стосовно цієї запропонованої зміни.

4. Комітет Міністрів розглядає запропоновану зміну та будь-який висновок, поданий Консультативним комітетом, і може затвердити зміну.

5. Текст будь-якої зміни, затвердженої Комітетом Міністрів відповідно до пункту 4 цієї статті, надсилається Сторонам для прийняття.

6. Будь-яка зміна, затверджена відповідно до пункту 4 цієї статті, набуває чинності на тридцятий день після того, як усі Сторони повідомили Генеральному секретарю про її прийняття.

Глава VII
Заключні положення

Стаття 22
Набуття чинності

1. Ця Конвенція відкрита для підписання Державами – членами Ради Європи. Вона підлягає ратифікації, прийняттю або схваленню. Ратифікаційні грамоти або документи про прийняття чи схвалення здаються на зберігання Генеральному секретарю Ради Європи.

2. Ця Конвенція набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати, коли п'ять Держав – членів Ради Європи висловили свою згоду на обов'язковість для них цієї Конвенції відповідно до положень попереднього пункту.

3. Для будь-якої Держави-члена, яка в подальшому висловить свою згоду на обов'язковість для неї цієї Конвенції, вона набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання ратифікаційної грамоти або документа про прийняття чи схвалення.

Стаття 23
Приєднання Держав, що не є членами Ради Європи

1. Після набуття чинності цією Конвенцією, Комітет Міністрів Ради Європи може запропонувати будь-якій Державі, яка не є членом Ради Європи, приєднатися до цієї Конвенції за допомогою рішення, що приймається більшістю голосів, передбаченою в пункті «d» статті 20 Статуту Ради Європи (994_001), і шляхом одностайного голосування представників Договірних Держав, які мають право засідати в Комітеті.

2. Для будь-якої Держави, що приєдналася до цієї Конвенції, Конвенція набуває чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретарю Ради Європи.

Стаття 24
Територіальні положення

1. Будь-яка Держава, під час підписання або здачі на зберігання своєї ратифікаційної грамоти або свого документа про прийнят-

тя, схвалення чи приєднання, може визначити територію або території, до яких застосовується ця Конвенція.

2. Будь-яка Держава може будь-коли після цього, шляхом подання заяви на ім'я Генерального секретаря Ради Європи поширити дію цієї Конвенції на будь-яку іншу територію, визначену в цій заяві. Конвенція набуває чинності стосовно такої території в перший день місяця, що настає після закінчення тримісячного періоду від дати отримання такої заяви Генеральним секретарем.

3. Будь-яка заява, зроблена відповідно до двох попередніх пунктів, може бути відкликана стосовно будь-якої території, визначеної в цій заяві, шляхом подання відповідного повідомлення на ім'я Генерального секретаря. Відкликання набуває чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 25
Застереження

Жодне застереження стосовно положень цієї Конвенції не дозволяється.

Стаття 26
Денонсація

1. Будь-яка Сторона може будь-коли денонсувати цю Конвенцію шляхом подання відповідного повідомлення на ім'я Генерального секретаря Ради Європи.

2. Така денонсація набуває чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 27
Повідомлення

Генеральний секретар Ради Європи повідомляє Державам-членам Ради Європи та будь-якій Державі, що приєдналася до цієї Конвенції, про:

a) будь-яке підписання;

b) здачу на зберігання будь-якої ратифікаційної грамоти чи будь-якого документа про прийняття, схвалення або приєднання;

c) будь-яку дату набуття чинності цією Конвенцією відповідно до статей 22, 23 та 24;

d) будь-яку іншу дію або повідомлення, що стосуються цієї Конвенції.

На посвідчення чого ті, що підписалися нижче, належним чином на те вповноважені, підписали цю Конвенцію.

Учинено в Страсбурзі 28 січня 1981 року англійською та французькою мовами, причому обидва тексти є автентичними, в одному примірнику, який зберігається в архівах Ради Європи. Генеральний секретар Ради Європи надсилає засвідчені копії цієї Конвенції кожній Державі-члену Ради Європи та будь-якій Державі, якій було запропоновано приєднатися до цієї Конвенції.

Публікації документа:

- **Офіційний вісник України** від 14.01.2011–2011 р., № 1 / № 58, 2010, ст. 1994 / стор. 701, стаття 85, код акту 54293/2011

Науково-практичне видання

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА ПРАКТИЧНІ АСПЕКТИ

Підписано до друку 12.12.2015. Формат 70x100/16.
Умов. друк. арк. 16,13. Папір офсетний. Друк офсетний.

Видавництво «К.І.С.»
04080 Київ–80, а/с 1, тел. (044) 462 5269
http://kis.kiev.ua
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи ДК №677 від 19.11.2001 р.