ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА ПРАКТИЧНІ АСПЕКТИ

НАУКОВО-ПРАКТИЧНИЙ ПОСІБНИК

Маркіян Бем
Іван Городиський

2021

Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини

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

Маркіян Бем,
Іван Городиський

2021

Ця публікація виготовлена за фінансової підтримки Європейського Союзу та Ради Європи. Погляди, викладені в цьому документі, не відображають офіційну позицію Європейського Союзу та Ради Європи.

Верстка, дизайн обкладинки та друк: «К.І.С.»

Фото: © Shutterstock

Council of Europe Publishing
F-67075 Strasbourg Cedex
(http://book.coe.int)

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ВРУ – Верховна Рада України

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

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

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

ККУ – Кримінальний кодекс України

КМ РЄ – Комітет міністрів Ради Європи

Конвенція 108+ – Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. (модернізована)

КУпАП – Кодекс України про адміністративні правопорушення

ООН – Організація Об'єднаних Націй

Порядок – Порядок здійснення Уповноваженим ВРУ контролю за додержанням законодавства про захист персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14

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

РЄ – Рада Європи

Типовий порядок – Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14

Уповноважений – Уповноважений Верховної Ради України з прав людини

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

1.1. Міжнародні документи

Міжнародно-правове регулювання має особливо важливе значення для закріплення та дієвості прав та свобод людини. Для багатьох із видів прав людини шлях до їх юридичного визнання та нормативного закріплення розпочався саме з міжнародних документів. Право на приватність (англ. *right to privacy*) багато в чому пройшло саме цей шлях, бувши визнаним спершу на міжнародному рівні й уже згодом імплементованим на рівні національного права.

Вперше нормативне закріплення норми з правового регулювання захисту персональних даних відбулося в тих положеннях міжнародних договорів з прав людини, які гарантували право на приватність. Зокрема, у Загальній декларації прав людини 1948 р., у ст. 12 встановлено, що: «Ніхто не може зазнавати безпідставного втручання в його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань»[1].

Згодом, це право було підтверджене та гарантоване у ст. 17 Міжнародного пакту про громадянські і політичні права від 1966 р., у якій закріплено, що: «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. Кожна людина має право на захист закону від такого втручання чи таких посягань»[2].

Водночас право на приватність, яке належить до прав людини першого покоління, перетворюється на універсальне, свого роду наскрізне право, яке вноситься і в зміст міжнародно-правових актів, які регламентували захист прав та свобод окремих груп або ж в окремих сферах. Зокрема, аналогічні до вищенаведених чи схожі за змістом положення внесені до Конвенції про права дитини 1989 р. (ст. 16), Міжнародної конвенції про захист прав усіх трудящих-мігрантів

1 Загальна декларація прав людини від 10.12.1948 р. *Голос України*. 2008. 10 груд. (№236).

2 Міжнародний пакт про громадянські і політичні права від 16.12.1966. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 30.04.2021).

та членів їхніх сімей 1990 р. (ст. 18), Конвенції про права осіб з інвалідністю 2006 р. (ст. 22) та ін.

Також розробляння міжнародних актів у сфері права на приватність та захисту персональних даних ведеться в рамках різних міжнародних організацій. Наприклад, в рамках Організації Об'єднаних Націй (надалі – ООН) 14 грудня 1990 р. Резолюцією Генеральної Асамблеї ООН №/95 (XLV) ухвалено Керівні принципи регламентації комп'ютеризованих картотек, що містять дані особистого характеру (англ. *Guidelines for the Regulation of Computerized Personal Data Files*).

Також варто відзначити діяльність Організації з економічного співробітництва та розвитку (надалі – ОЕСР), в рамках якої розроблено «Базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних» (англ. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*), схвалені Рекомендацією Ради ОЕСР від 23 вересня 1980 р., нова редакція яких була ухвалена у 2013 р. Крім міжнародних договорів з прав людини, ухвалених на універсальному рівні, відповідні норми внесені у зміст міжнародних договорів, укладених у рамках регіональних систем захисту прав людини. Наприклад, положення щодо захисту права на приватність містяться в ст. 11 Американської конвенції з прав людини 1969 р. (ст. 11), ст. 7 Хартії основних прав Європейського Союзу 2000 р. (с. 7) та ін. Особливо широкі відповідні гарантії та практика щодо їх застосування та захисту в рамках системи Ради Європи.

Особливо варто відзначити ті міжнародні документи, що стосуються захисту персональних даних, які укладено в рамках європейського правового простору, під егідою Ради Європи та Європейського Союзу. Ми детальніше розглянемо їх в дальшому підрозділі.

1.2. Акти Ради Європи та Європейського Союзу

4 листопада 1950 року десять європейських держав у м. Римі підписали Конвенцію про захист прав людини і основоположних свобод (далі – Конвенція). Вказаним документом передбачено низку прав та свобод, які держави – учасниці Конвенції повинні гарантувати кожному, хто перебуває під їхньою юрисдикцією. Зокрема, статтею 8 Конвенції передбачено:

«1. Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції.

2. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської

безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб»[3].

Також з метою дотримання державами-учасницями взятих на себе зобов'язань за Конвенцією нею передбачено створення Європейського суду з прав людини (далі ЄСПЛ, Європейський суд або Суд). Саме Суд, згідно з частиною 1 статтею 37 Конвенції, своїми рішеннями тлумачить та застосовує Конвенцію та Протоколи до неї та визначає так обсяг гарантованих ними прав. З огляду на те, що ЄСПЛ тлумачить положення Конвенції в світлі реалій сьогодення, для того щоб забезпечити їх дієвість та практичність, не дивно, що обсяг вказаних прав та сфера застосування Конвенції з часом помітно розширюються.

Наприклад, аналізуючи у справі «*Leander v. Sweden*» скарги на порушення статті 8 Конвенції у зв'язку з обробкою правоохоронними органами персональних даних заявника, ЄСПЛ у своєму рішенні зазначив, що «Ніким не заперечується, що таємна база даних поліції містила відомості щодо приватного життя п. Леандера. Як зберігання, так і розкриття такої інформації, поєднані з відмовою надати п. Леандеру можливості заперечити її, становили втручання в його право на повагу до приватного життя, гарантоване частиною 1 ст. 8»[4]. Отже, у вказаному рішенні, ухваленому 1987 року, ЄСПЛ уперше чітко вказав, що 1) зберігання та розкриття 2) державним органом 3) **інформації про приватне життя особи**, може розцінюватися як втручання в її право на повагу до приватного життя, гарантоване частиною 1 ст. 8 Конвенції. Тому, щоб не порушувати вказаного положення Конвенції, відповідне втручання з боку держави повинно відповідати вимогам, викладеним у частині 2 ст. 8 Конвенції, тобто: 1) здійснюватися «згідно із законом»; 2) переслідувати одну з легітимних цілей, перелічених у частині 2 ст. 8 Конвенції; та 3) бути «необхідним» для досягнення такої цілі. Відтоді ті чи інші питання обробки персональних даних регулярно стають предметом звернення до ЄСПЛ, а напрацьована ним у цій частині практика – невіддільна частина правового регулювання питання обробки персональних даних.

Наприклад, уже в одному з подальших рішень з цього приводу у справі «*Amann v. Switzerland*»[5] [GC] Суд, у контексті дослідження питання обробки інформації про особу, надав визначення того, що він має на увазі під «**приватним життям**», вказавши, що воно охоплює не лише 1) право жити приватно, поза межами небажаної уваги (англ. *the right to live privately, away from unwanted attention*), а й 2) право встановлювати та розвивати відносини з іншими людьми, що,

3 Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 р. Голос України. 2001. 10 січ. (№3).

4 *Leander v. Sweden*, п. 48. Тут і надалі по тексту вказуватимуться лише назви справ. Детальніша інформація щодо рішення в кожній із використаних справ міститься в переліку рішень ЄСПЛ, що додаються до цього посібника (*Прим. авт*).

5 *Amann v. Switzerland*, п. 65.

своєю чергою, охоплює професійну діяльність та соціальне життя людини[6]. Тому і вся інформація, яка стосується вказаних сфер життя людини, така, що охоплюється гарантованим статтею 8 Конвенції правом на повагу до приватного життя. Отже, Суд з часом зближує поняття інформації про приватне життя особи з **поняттям персональних даних**.

У подальшому сфера дії вказаного положення була суттєво розширена ЄСПЛ і станом на сьогодні охоплює як питання обробки державою персональних даних особи, так і (опосередковано) певні аспекти обробки персональних даних приватними суб'єктами. Наприклад, Суд вказав, що за певних умов держава повинна вживати розумних заходів з метою забезпечення дотримання права особи на повагу до її приватного життя з боку приватних суб'єктів. Перелік ключових рішень ЄСПЛ щодо захисту персональних даних та права на приватність міститься в Додатку № 1.

28 січня 1981 року ухвалено Конвенцію № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (далі – Конвенція 108). У цьому документі вперше викладено ключові принципи обробки персональних даних, права особи у зв'язку з обробкою її персональних даних, базові норми щодо транскордонної передачі даних, а також передбачено створення консультативного комітету, до чиїх обов'язків входило проведення аналізу того, як застосовується Конвенція 108, та в разі необхідності підготування пропозицій щодо внесення змін до Конвенції 108[7].

У подальшому, а саме 8 листопада 2001 р., ухвалено Додатковий протокол до цього міжнародного договору, який деталізував положення Конвенції № 108 у частині, що стосується транскордонної передачі даних, та містив нові положення щодо необхідності створення сторонами Конвенції наглядового органу, який би вів контроль за додержанням законодавства про захист персональних даних на національному рівні[8].

Сильні сторони вказаного документа – те, що він застосовується до всіх сфер обробки персональних даних, як у публічному, так і в приватному секторі. Отже, Конвенція № 108 охоплює низку надчутливих питань, які виходять за межі правового регулювання прогресивнішого законодавства з питань захисту персональних даних Європейського Союзу, як, наприклад, негласне спостереження, правоохоронна діяльність тощо.

Також вказаний документ відкритий для підписання державами, що не члени Ради Європи. Станом на сьогодні серед сторін Конвенції № 108 є Аргентина, Маврикій, Марокко, Уругвай, Мексика, Туніс, Сенегал та Кабо-Верде.

---

6 *Bărbulescu v. Romania*, п. 70.

7 Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. – *Офіційний вісник України*. 2011. 14 січ. (№ 58). Ст. 701.

8 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 року. *Офіційний вісник України*. 2011. 14 січ. (№ 1(58)).

Після ухвалення Конвенції № 108 Комітет міністрів Ради Європи (далі – КМ РЄ) вів активну роботу в напрямку роз'яснення порядку застосування її положень у ході проведення обробки персональних даних у сферах, де наявний найбільший ризик порушення прав людини. З цією метою КМ РЄ ухвалив низку рекомендацій щодо обробки персональних даних у таких чутливих щодо цього сферах, як соціальний захист, страхування, охорона здоров'я, правоохоронна діяльність, інтернет та ін.[9]. Ці рекомендації сприяють підтриманню положень Конвенції № 108 в актуальному стані. Вичерпний перелік рекомендацій КМ РЄ з питань захисту персональних даних викладено в Додатку № 2.

2011 року з огляду на нові виклики, пов'язані з швидким розвитком технологій, КМ РЄ ухвалив рішення щодо початку роботи над оновленням Конвенції № 108. Початково робота в цьому напрямку була доручена консультативному комітетові за Конвенцією № 108, а в подальшому – спеціально створеному з цією метою міжурядовому комітетові – CAHDATA (англ. *ad hoc Committee on data protection*), який розпочав роботу 2013 року. Роботу Комітету завершено у 2016 році і її результати передано на розгляд КМ РЄ, який 18 травня 2018 року своїм рішенням прийняв додатковий протокол до Конвенції № 108[10]. Вказаний документ був відкритий до підписання сторонами 10 жовтня 2018 року. Станом на сьогодні Додатковий протокол ще не набув чинності. Україна вказаний документ ще не підписала.

Серед нововведень, запроваджених Додатковим протоколом, можна виділити такі:

- запроваджено поняття розпорядника персональних даних;
- поняття автоматизованої обробки персональних даних замінено на обробку персональних даних. Таким чином Конвенція 108+ застосовуватиметься до обробки даних, як за допомогою автоматизованих систем, так і вручну;
- Конвенція 108+ не застосовуватиметься до обробки персональних даних фізичними особами для особистих чи побутових потреб;

9 Зокрема, з останніх ухвалених рекомендацій Комітету міністрів: Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems; Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data; Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfill the rights of the child in the digital environment; Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries; Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests та ін. *(Прим. авт.)*

10 Часто Конвенцію № 108 з урахуванням змін, які запроваджуються Додатковим протоколом, ухваленим 18 травня 2018 року, називається «модернізована Конвенція 108» або Конвенція № 108+. Саме так вона називатиметься в цьому посібнику надалі. (*Прим. авт.*)

- держави-сторони повинні ухвалити законодавство, яке б запроваджувало на національному рівні положення Конвенції 108+, а консультативний комітет відтепер володітиме повноваженнями перевіряти, чи були дотримані вказані вимоги;
- передбачено можливість приєднання до Конвенції 108+ міжнародних організацій та ЄС;
- Конвенція 108+ детальніше викладає принцип пропорційності. Ніякі відступи від вказаного принципу, а також від принципу законності, не допускаються;
- запроваджуються деталізовані підстави обробки персональних даних: згода (яка повинна бути добровільною, конкретною, поінформованою та однозначною) або інша, передбачена законом підстава;
- розширено перелік чутливих даних (генетичних, біометричних, щодо етнічного походження та належності до профспілок);
- обов'язок володільців повідомляти наглядовий орган про такі порушення режиму захисту персональних даних, які можуть становити серйозне втручання в права суб'єктів персональних даних;
- запроваджено обов'язок володільця повідомляти суб'єкта персональних даних визначений ч. 1 ст. 8 Конвенції 108+ обсяг інформації щодо обробки його персональних даних;
- розширено перелік прав суб'єкта персональних даних;
- запроваджується низка обов'язків володільців та розпорядників персональних даних: зокрема бути здатним продемонструвати дотримання в ході обробки вимог Конвенції 108+, аналізувати, яким буде вплив планованої обробки персональних даних на права суб'єктів перед її початком, організувати обробку так, щоб мінімізувати ризики втручання в ці права (захист персональних даних за планом); запровадити технічні та організаційні заходи, що враховували б правила обробки даних на всіх етапах обробки (захист персональних даних за замовчуванням);
- запроваджуються деталізовані положення щодо транскордонної передачі персональних даних, покликані, серед іншого, забезпечити, щоб персональні дані, які передаються отримувачам з інших юрисдикцій (не держав-сторін), користувалися рівнем захисту, що відповідає тому, що передбачений Конвенцією 108+ та ін.[11].

Отже, прийняття державами Конвенції № 108+ буде значним кроком вперед, якщо порівняти з Конвенцією № 108. Разом з тим варто відзначити, що значна

11 Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data) of 18th May, 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Date of request: 2021).

частина вказаних положень Конвенції № 108+ вже внесені в національне законодавство, яке значною мірою будувалося на основі правового регулювання Європейського Союзу.

Саме Європейський Союз сьогодні став локомотивом розвитку правового регулювання у сфері захисту персональних даних. Ключове місце права на приватність серед спільних європейських цінностей було підтверджене і в Хартії основних прав ЄС від 7 грудня 2000 р. У Хартію внесено як ст. 7, що гарантувала право на приватність, так і ст. 8, що встановлювала гарантії «Захисту відомостей особистого характеру». Ця стаття передбачає, що такі відомості «повинні використовуватися відповідно до встановлених правил для певних цілей і на підставі згоди зацікавленої особи або на інших правомірних підставах, передбачених законом». Крім того, ст. 8 гарантувала право на доступ до своїх персональних даних та право на їх виправлення, а також передбачала, що відповідний захист має підлягати контролеві з боку незалежного органу[12].

До недавнього часу 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) була не просто одним із найавторитетніших документів у сфері захисту персональних даних була, а й зразком для багатьох національних законів про захист персональних даних за межами ЄС. Не став винятком і Закон України «Про захист персональних даних».

«Євроорієнтованість» національного законодавства про захист персональних даних обумовлюється тим, що співробітництво в цій сфері визначено одним з ключових елементів поглиблення співпраці між Україною та ЄС в інших сферах. Наприклад, Угода про асоціацію між Україною та ЄС містить ст. 15 «Захист персональних даних», згідно з якою «Сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних *відповідно до найвищих європейських та міжнародних стандартів*».

Попри те, що Директива була одним з найпрогресивніших документів у сфері захисту персональних даних у світі, технологічний прогрес та зростання обсягів автоматизованої обробки персональних даних зумовили виникнення нових викликів та проблем у цій сфері, які потребували додаткової правової регламентації. Зокрема, активний розвиток таких гігантів як «Фейсбук» чи «Альфабет» («Гугл») невідривно пов'язаний із відстежуванням активності користувачів та обробкою їхньої персональної інформації, що приводило до зростання їхньої власної прибутковості з одночасним збільшенням ризиків для суб'єктів персональних даних.

Через це з'явилася потреба в розробленні нового регулювання на рівні Європейського Союзу, яке б доповнювало і розширювало зміст Директиви, встановлювало додаткові гарантії для суб'єктів і вимоги до володільців і

12 Хартія основних прав Європейського Союзу від 07 грудня 2000 р. URL: https://zakon.rada.gov.ua/laws/show/994_524#Text (Дата звернення: 30.04.2021).

розпорядників персональних даних. Його розроблення стало можливим після укладення Лісабонського договору 2007 р., який вніс зміни в установчі договори ЄС. Стаття 16 Договору про функціонування ЄС в редакції Лісабонського договору підтверджує, що «кожен має право на захист своїх персональних даних» і передбачала право Європейської Ради та Парламенту встановлювати спільні правила обробки персональних даних для всіх держав – членів ЄС.

Дискусія щодо необхідності спільного загальноєвропейського регулювання обробки та захисту персональних даних розпочалася 2009 р. з ініціативи Європейської комісії. Документом, який встановив таке регулювання, став Загальний регламент про захист персональних даних (англ. *General Data Protection Regulation, GDPR*, надалі – Регламент). Європейська комісія опублікувала його проєкт з метою обговорення в січні 2012 р., ухвалення на рівні ЄС відбулося 14 квітня 2016 р., а набрання чинності – 25 травня 2018 р.

Цей документ складається з 11 розділів та 99 статей та супроводжується 173 коментарями (англ. *Recitals*). Серед головних особливостей юридичної дії Регламенту можна виділити такі:

- його дія поширюється на всіх громадян держав – членів ЄС, а також резидентів ЄС, незалежно від їхнього громадянства;
- територіальна дія Регламенту поширюється на територію як держав – членів ЄС, так і держав, що входять до Європейської економічної зони (Норвегія, Ісландія та Ліхтенштейн);
- Регламент – акт прямої дії, він загальнообов'язковий та застосовується державами – членами ЄС без додаткового ухвалення внутрішніх нормативних актів.

Говорячи про головні змістовні новели цього правового акта, якщо порівняти з Директивою ЄС, Регламент визначає правила гри для всіх учасників процесу захисту та обробки персональних даних – як суб'єктів, так і для володільців і розпорядників та контрольних органів у цій сфері. Зокрема, документ містить повний каталог прав суб'єктів персональних даних, які були раніше закріплені в Директиві та Хартії та розширює їхній зміст (розділ 3)[13].

Щодо організацій, які проводять обробку персональних даних як володільці та розпорядники, то до них встановлено вимогу гарантувати, що в разі автоматизованої обробки персональних даних інформаційні системи та програмне забезпечення за замовчуванням (англ. *by default*) забезпечують їхній захист (ст. 25), у разі необхідності призначати в організації уповноваженого із захисту

13 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 23.05.2021 р.).

персональних даних (англ. *Data Protection Officer,* ст. 37–39) та відповідного представника в ЄС, якщо організація зареєстрована та має центр ухвалення рішень за межами ЄС (ст. 27), положення щодо співпраці з контрольними органами держав – членів ЄС у разі витоку персональних даних (англ. *data breach*, ст.ст. 31, 33–34), санкції, зокрема штрафи, за порушення правил Регламенту (розділ 8) та ін.[14].

Важливі також положення, які регламентують діяльність незалежних контрольних органів щодо захисту персональних даних, які повинні діяти в держав-членах ЄС, правила їх створення та компетенції (ст.ст. 51–59). Слід окремо відзначити правила транскордонної передачі персональних даних, що містяться в розділі 5, що де-факто розширює суб'єктну сферу дії Регламенту, спонукаючи організації з третіх держав, які ведуть діяльність з обробки особистої інформації громадян та резидентів ЄС, дотримуватися його положень[15].

Ухвалення Регламенту та насамперед його зміст, істотно змінили ландшафт захисту персональних даних у Європі та у світі. Як відзначав засновник «Фейсбуку» Марк Цукерберг у ході слухань у Сенаті США у квітні 2018 р., ухвалення Регламенту було правильним кроком і США теж варто обдумати ухвалення схожого правового акта. Детальніше його зміст буде проаналізований у цьому посібнику нижче.

Дуже часто Регламент зазнає критики у зв'язку з начебто надмірною суворістю його положень, що ускладнює обробку персональних даних у комерційній, творчій, науковій та інших сферах. Водночас європейські експерти слушно наголошують, що цей акт «створює єдині узгоджені правила захисту персональних даних для всього Європейського Союзу, встановлюючи простір юридичної визначеності, з якого мають користь як суб'єкти економічної діяльності, так і фізичні особи – суб'єкти персональних даних»[16].

---

14 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 23.05.2021 р.).

15 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 23.05.2021 р.).

16 Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. С. 34.

1.3.Національне законодавство України

На національному рівні ключові документи у сфері захисту персональних даних – Конституція України, Закон України «Про захист персональних даних» (далі – Закон) та документи у сфері захисту персональних даних, ухвалені Уповноваженим Верховної Ради України з прав людини. Вагоме значення має також низка інших законів, як, наприклад, Закон України «Про доступ до публічної інформації» та Закон України «Про інформацію». Разом з тим практично всі галузеві нормативно-правові акти також містять положення, що регламентують обробку персональних даних у відповідній сфері.

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[17].

Положення цієї статті роз'яснено в рішенні Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 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 погляду 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» (т. зв. «Справа К. Г. Устименка»).

З метою імплементації Конвенції 108 Верховна Рада України 1 червня 2010 р. ухвалила Закон України «Про захист персональних даних», який закріплює основні принципи обробки персональних даних, права суб'єктів персональних даних, підстави обробки персональних даних, підстави обробки чутливих категорій персональних даних, принципи обмеження дії Закону, повноваження наглядового органу та ін.[18].

На виконання Закону наглядовий орган у сфері захисту персональних даних – станом на сьогодні це Уповноважений Верховної Ради України з прав людини – наказом від 8 січня 2014 року № 1/02-14 затвердив низку підзаконних актів у сфері захисту персональних даних:

17 Конституція України від 28 червня 1996 р. №254к/96-ВР. *Голос України*. 1996. 13 лип. (№128).

18 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№122).

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

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

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

Детальніше вказані документи проаналізовані нижче у відповідних розділах, де розкриваються питання, що належать до сфери їх правового регулювання.

Також вагоме значення у сфері захисту персональних даних мають норми, якими встановлюється відповідальність за порушення законодавства про захист персональних даних.

Наприклад, ст. 182 Кримінального кодексу України («Порушення недоторканності приватного життя») передбачено відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації[19].

Також ст. 188-39 Кодексу України про адміністративні правопорушення (КУпАП) («Порушення законодавства у сфері захисту персональних даних») передбачено відповідальність за низку порушень Закону України «Про захист персональних даних», зокрема 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»[20].

Крім цього, положення Закону мають подальше роз'яснення в рішеннях судів, ухвалених за результатами розгляду складених працівниками Секретаріату Уповноваженого ВРУ з прав людини протоколів про скоєння адміністративного правопорушення, передбаченого ст. 188-39 КУпАП.

Нижче у відповідному розділі детальніше проаналізовано те, як вказані норми про відповідальність за порушення законодавства про захист персональних даних застосовуються на практиці, та які види порушень тягнуть за собою передбачену вказаними нормами відповідальність.

---

19 Кримінальний кодекс України : Закон України від 5 квітня 2001 р. *Відомості Верховної Ради України*. 2001. № 5. Ст. 131.

20 Кодекс України про адміністративні правопорушення : Закон України від 18 грудня 1984 р. *Відомості Верховної Ради УРСР*. 1984. № 40. Ст. 1122.

Окремо варто наголосити на важливій ролі у сфері обробки персональних даних низки інших, дотичних до цієї сфери нормативно-правових актів.

Насамперед ідеться про Закон України «Про доступ до публічної інформації». Згідно з його ст. 1, «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. **Публічна інформація є відкритою, крім випадків, встановлених законом**»[21].

Безперечно, що значна кількість публічної інформації містить персональні дані. З огляду на вказане означення публічної інформації, цим поняттям охоплюються величезні масиви персональних даних. Ідеться про інформацію, що перебуває у володінні суб'єктів владних повноважень та деяку інформацію, що перебуває у володінні юридичних осіб публічного та приватного права. Тому постає запитання щодо того, як повинна вестися обробка (зокрема, поширення) таких персональних даних і як узгодити в цій частині положення Закону України «Про захист персональних даних», з одного боку, та Закону України «Про доступ до публічної інформації» – з іншого. У цьому зв'язку слід звернутися до Закону України «Про доступ до публічної інформації», який містить релевантніші положення з цього приводу. Зокрема, йдеться про ч. 2 ст. 6 вказаного Закону, якою передбачено, що при розв'язанні питання про те, чи обмежувати доступ до конфіденційної інформації (яка містить персональні дані (див. детальніші відомості з приводу цього питання нижче) слід застосувати передбачений вказаним положенням Закону *трискладовий тест*[22]. Аналіз, який необхідно провести, користуючись вказаним тестом, містить у собі всі ключові вимоги Закону України «Про захист персональних даних» та при строгому дотриманні забезпечує неухильне додержання його вимог при розв'язанні питання щодо (не)надання публічної інформації, яка містить персональні дані.

Крім цього, ст. 10 Закону України «Про доступ до публічної інформації» містить норми щодо прав суб'єктів персональних даних та обов'язків володільців персональних даних (в розумінні Закону України «Про доступ до публічної

21 Про доступ до публічної інформації : Закон України від 13 січня 2011 р. №2939-VI. *Голос України*. 2011. 09 лют. (№24).

22 Обмеження доступу до інформації відбувається відповідно до закону при дотриманні сукупності таких вимог:
1) лише в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, 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. *(Прим. авт.)*

інформації» – розпорядників) у контексті роботи з публічною інформацією, що містить персональні дані[23]. Вказані положення, хоч і здебільшого дублюють положення Закону України «Про захист персональних даних», водночас підсилюють їх значення в роботі розпорядників публічної інформації.

Також Закон України «Про інформацію» та низка інших нормативно-правових актів, що регламентують роботу ЗМІ, визначають, як повинні оброблятися персональні дані в указаній сфері. Це питання детально проаналізовано в дальшому розділі.

На завершення, варто зазначити, що Закон України «Про захист персональних даних» – рамковий документ. Його положення регулюють правові відносини, пов'язані із захистом та обробкою персональних даних у величезній кількості сфер суспільного життя. З цих же причин Закон не може детально визначати порядок та процедуру обробки персональних даних у всіх вказаних сферах. У зв'язку з цим кожна галузь права містить (і повинна містити) свої положення, які регламентують особливості обробки персональних даних у відповідній сфері суспільних відносин.

Наприклад, Кримінальний процесуальний кодекс України та Закон України «Про оперативно-розшукову діяльність», закони, що регулюють роботу тих чи інших правоохоронних органів (Національної поліції, Служби безпеки України, Державного бюро розслідувань та ін.), а також закони (скажімо., «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус») та підзаконні нормативно-правові акти[24], що регламентують ведення тих чи інших реєстрів, баз даних та ін., визначають деталі обробки персональних даних у сфері правоохоронної діяльності. Аналогічним чином влаштовано процес обробки персональних даних і в інших сферах суспільного життя.

У цьому зв'язку варто наголосити, що в частині, яка стосується питань обробки персональних даних, вказані документи завжди повинні узгоджуватися зі ст. 32 Конституції та Законом України «Про захист персональних даних», які визначальні в цій сфері правових відносин.

---

23 Про доступ до публічної інформації : Закон України від 13 січня 2011 р. №2939-VI. *Голос України*. 2011. 09 лют. (№24).

24 Наприклад, Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : Наказ Міністерства внутрішніх справ України від 12.10.2009 N 436. *Офіційний вісник України*. 2010. 11 січ. (№101). Ст. 409.

2. ЗМІСТ КЛЮЧОВИХ ТЕРМІНІВ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Поняття «персональні дані»

Означення та розуміння поняття «персональні дані» – одне з найважливіших при роботі в цій сфері. У Регламенті, Директиві, Конвенції та Законі поняття персональних даних означено приблизно однаково, а саме: «будь-яка інформація, яка стосується ідентифікованої особи або особи, яка може бути ідентифікованою».

Якщо з ідентифікованою особою все більш-менш зрозуміло, то поняття «*особи, яка може бути ідентифікованою*» потребує додаткових роз'яснень. Ідентифікована – особа, яку за наявною в розпорядженні володільця інформацією можна безпомилково виділити з-посеред інших осіб. Зазвичай для того, щоб вважати особу ідентифікованою, необхідні її ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу/цифровий номер, що присвоюється особі (наприклад, ідентифікаційний номер фізичної особи).

Однак за певних умов наявність меншої кількості інформації чи певного обсягу іншої інформації достатньо для того, щоб особу вважати такою, «*яка може бути ідентифікованою* «.

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

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

Приклад 3. Компанія, що володіє медичними даними пацієнтів, розділяє дані щодо стану здоров'я та особисті дані особи, що дають змогу її ідентифікувати. При цьому використовується шифр,

який присвоюється вказаним групам даних та в разі потреби надасть можливість встановити, кому з пацієнтів належать медичні дані. Знеособлені так відомості щодо стану здоров'я передаються іншій компанії для проведення наукових досліджень. У цьому випадку провести ідентифікацію буде практично неможливо, через заходи із знеособлення.

Більше деталей щодо цього передбачає Регламент. Вказаний документ містить найсучасніше та найпрактичніше означення «особи, що може бути ідентифікованою», згідно з яким це «особа, яку можна ідентифікувати прямо чи опосередковано, зокрема вказавши такі ідентифікатори, як ім'я, ідентифікаційний номер, дані щодо місцезнаходження, онлайн ідентифікатор чи інші особливості фізичної, фізіологічної, генетичної, духовної, економічної, культурної чи соціальної ідентичності такої фізичної особи».

Отже, коли йдеться про «*особу, яка може бути ідентифікованою*» очевидно, що мається на увазі не лише встановлення її особи за іменем та іншими «класичними» ознаками, а й безпомилкове виділення її з невизначеного кола інших осіб за допомогою сукупності наявних відомостей. Часто мається на увазі ідентифікація особи на базі відомостей, які, якщо взяті окремо, не дають можливості ідентифікувати особу, однак у поєднанні уможливлюють це. Також вагомий елемент тут те, як складно ідентифікувати таку особу, адже якщо ідентифікувати можна, однак це коштуватиме значних затрат часу, грошей, зусиль тощо, то, звісно, за таких умов особа не можна вважати такою, «*яка може бути ідентифікованою*».

Вказані критерії, хоч і не прямо, закладені й у національному Законі. Тож видається доцільним саме в такому річищі тлумачити його положення.

Щодо **класифікації персональних даних**, слід зазначити, що як Законом (ст. 7), так і Директивою (ст. 8), Регламентом (ст. 9) та Конвенцією (ст. 6) із загального переліку персональних даних виділяються спеціальні (також їх часто характеризують, як чутливі) категорії персональних, обробка яких дозволяється лише в 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 і професійних спілках;
- засудження до кримінального покарання;
- стан здоров'я, статеве життя;
- біометричні або генетичні дані.

Обробка цих категорій персональних даних повинна відбуватися лише у виняткових випадках із забезпеченням вищих стандартів як захисту, так і дотримання прав суб'єктів персональних даних.

В основі такого поділу лежить те, що вказані категорії персональних даних мають у собі інформацію щодо ознак, які часто можуть стати підставою для дискримінаційного ставлення до відповідного суб'єкта персональних даних. Неважко уявити, якими б могли бути наслідки, якби, наприклад, роботодавець міг без жодної потреби вимагати в потенційних кандидатів на посаду вказувати відомості щодо їхнього расового чи етнічного походження або релігійних переконань в анкеті чи резюме, що вони направляють з метою працевлаштування. Отже, мета виділення спеціальних категорій персональних даних – забезпечення того, щоб їх обробка проводилася лише у разі виняткової необхідності.

2.2. Поняття «обробка персональних даних»

Відповідно до Закону, обробка персональних даних – це «будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем»[25].

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

Слід зазначити, що в Законі, поруч із терміном «обробка», паралельно застосовуються й інші терміни, використання яких викликає деякі сумніви щодо їх правильності. Зокрема, йдеться про поняття «використання» та «захист» і їх співвідношення з поняттям «обробка». У цьому зв'язку слід звернути увагу на положення ст. 2 та ст. 10 Закону. Згідно з ч. 1 ст. 10 Закону, «**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

25 Про захист персональних даних : Закон України від 23.04.2021 р. №2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

даних чи відповідно до закону». При цьому, згідно зі ст. 2 Закону, «**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»[26].

Щодо захисту персональних даних , то його означення взагалі немає в Законі. Тож виникає суперечність:

Ст. 2 Закону	Обробка **включає** використання. Захист **не є** елементом обробки.
Ст. 10 Закону	Використання **включає** в себе обробку та захист.

Відповідно до усталеної практики Ради Європи та Європейського Союзу, захист не елемент обробки, бо не передбачає вчинення якихось дій з персональними даними. Використання зазвичай елемент обробки, однак інколи (наприклад, у Німеччині) використання – окрема відносно обробки дія щодо персональних даних. При цьому за жодної умови обробка не може бути елементом використання. Відповідно, «захист» персональних даних слід розглядати як дію, окрему від їх «обробки» та «використання», а «використання» – як один з елементів «обробки».

З огляду на те, що Закон містить неправильне означення вказаних термінів, видається доцільним у майбутньому впорядкувати вказані питання та привести понятійний апарат до «єдиного знаменника».

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

Передовсім, згідно з ч. 2 ст. 1, «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»[27]. Положення аналогічного змісту міститься і в ч. 1 ст. 2 Регламенту. У відповідному роз'ясненні до вказаного положення Регламенту (Recital 15 «Technology Neutrality») йдеться про те, що захист фізичних осіб повинен застосовуватися до обробки персональних засобів автоматизованими

26 Про захист персональних даних : Закон України від 23.04.2021 р. №2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

27 Про захист персональних даних : Закон України від 23.04.2021 р. №2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

засобами, а також до обробки «вручну» (*manual processing*), якщо персональні дані внесені або призначені для внесення до картотеки (*filing system*)[28].

Тож вказане положення залишає у сфері дії Закону лише такі види обробки:

1) обробку, що ведеться повністю або частково із застосуванням автоматизованих засобів. Тому будь-яка обробка із застосуванням, наприклад, комп'ютерів потрапляє у сферу дії Закону;

2) обробку персональних даних у картотеці;

3) обробку персональних даних, які поки не внесені в картотеку, однак призначені для цього.

Отже, неавтоматизована обробка персональних даних поза межами картотеки не охоплюється положеннями Закону.

Також, згідно з ч. 2 та ч. 3 ст. 25 Закону, його положення не застосовуються до:

- для приватних цілей;
- журналістських цілей;
- творчих цілей;

Обробка персональних даних для приватних цілей. Наприклад, ведення особою телефонної книги належить до приватних цілей. Однак, якщо ця особа – власник бізнесу (наприклад, ресторанів чи магазинів) і збирає персональні дані клієнтів (ім'я, прізвище, по батькові і номер телефона/адреса проживання) для використання з комерційною метою, як-от реклама та просування власних послуг, то це вже не можна вважати обробкою для приватних цілей, дарма що виконує її окрема особа для потреб власного бізнесу.

На ***обробку персональних даних для журналістських та творчих цілей*** 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 до сфери дії Закону. Однак, якщо втручання в право особи на повагу до приватного життя внаслідок обробки її персональних даних журналістами надмірне, якщо порівняти з суспільним інтересом до висвітленої інформації (персональних даних особи) чи її суспільною вагою, можуть порушуватися питання додержання законодавства про захист персональних даних.

28 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 23.05.2021 р.).

Приклад. На вебсайті одного із засобів масової інформації була викладена інформація щодо осіб, які не з'явилися до військового комісаріату після вручення їм повістки.

Висвітлення такої інформації – очевидний приклад порушення балансу між суспільними інтересами та правом окремої особи на захист її приватності. Дійсно, ухилення від військової служби, тоді як держава перебуває в стані збройного конфлікту, – суспільно вагома тема. Однак оприлюднення персональних даних вказаних осіб жодним чином не сприяло висвітленню цієї тематики, достатньо було навести звичайну статистичну інформацію. Натомість абсолютно очевидно, що адміністрація сайту переслідувала мету стигматизації цих осіб як таких, що в тяжкий для держави час ухиляються від виконання свого військового обов'язку. Тому така обробка персональних даних повинна відповідати положенням Закону, що за цих обставин (нема легітимної мети та законних підстав поширення персональних даних призовників) майже автоматично становитиме його порушення.

Наприклад, цілий пласт рішень ЄСПЛ присвячено діяльності ЗМІ, зокрема в частині поширення інформації, що містить персональні дані. У таких випадках ЄСПЛ зважує гарантоване ст. 10 Конвенції право на свободу висловлення думки, з одного боку, і гарантоване ст. 8 Конвенції право на повагу до приватного життя – з іншого. У рішеннях ЄСПЛ з цього приводу детально аналізується питання, про те, чи був забезпечений баланс між правом на повагу до особистого життя та правом на свободу вираження поглядів. Як уже зазначено вище, від розв'язання цього питання власне і залежить, чи застосовуватиметься Закон до обробки персональних даних для «*журналістських та творчих цілей*».

Розв'язуючи питання про те, чи був дотриманий вказаний баланс між правами, гарантованими ст. 8 та ст. 10 Конвенції, ЄСПЛ аналізує такі питання:

1) **внесок матеріалу (публікації) в дискусію, що становить публічний інтерес;**
2) **ступінь відомості/публічності особи, якої стосується відповідна інформація;**
3) **предмет опублікованого матеріалу;**
4) **попередня поведінка особи (якої стосується інформація);**
5) **а) зміст; б) форма; та в) наслідки публікації для особи, якої вона стосувалась;**

6) де потрібно – **умови, за яких були отримані фотографії** (таке формулювання використано в рішенні у справі *«Фон Ганновер проти Німеччини (№ 2)»*, де мова здебільшого йшла про оприлюднення фотографій. У справі *«Аксель Шпрінгер АГ проти Німеччини»*, де йдеться більше про висвітлення інформації в статті цей критерій сформульовано як **«спосіб отримання інформації та її правдивість»**);

7) щодо справ, розглядуваних за ст. 10 (тобто, де мова йде переважно про притягнення журналістів до відповідальності за поширення інформації), ЄСПЛ додає ще один критерій, а саме: **тяжкість санкції, застосованої щодо журналіста чи видавця.**

Вказані критерії були викристалізувані ЄСПЛ в його рішеннях у справах «*Von Hannover v. Germany (no. 2)*», «*Axel Springer AG v. Germany*» та «*Couderc and Hachette Filipacchi Associés v. France*» (див. приклади нижче). Що цікаво, рішення у справах «*Von Hannover v. Germany (no. 2)*» та «*Axel Springer AG v. Germany*» ухвалила Велика палата ЄСПЛ в один день. Перше з указаних рішень стосувалося скарг заявниці за ст. 8 Конвенції на поширення ЗМІ інформації щодо її особистого життя, а друге – скарг власника газети за ст. 10 Конвенції на притягнення його до відповідальності за поширення матеріалу щодо приватного життя відомого актора. У цьому зв'язку ЄСПЛ зазначив, що «*у справах… що вимагають зважування права на повагу до приватного життя супроти права на свободу слова, Суд вважає, що результат заяви теоретично не повинен змінюватися залежно від того, чи подавала її до Суду за ст. 8 Конвенції особа, яка була об'єктом статті, чи видавець – за ст. 10. Ці права заслуговують на однакову повагу*». Отже, і критерії до таких категорій справ застосовуються одні і ті ж (див. вище).

Приклад 1. Рішення ЄСПЛ у справі «Von Hannover v. Germany (no. 2)»

Фабула справи. Одне з відомих німецьких видань надрукувало статтю про те, що князь Монако Реньє III перебував у тяжкому стані і лише його молодша донька Стефані залишилася доглядати за ним, тоді як двоє інших дітей займалися своїми справами: принц Альберт брав участь в Олімпійських іграх у Солт-Лейк-Сіті, а заявниця (принцеса Кароліна фон Ганновер – дочка князя) із чоловіком, відпочивали на гірськолижному курорті у Сент-Моріці. У статті містився фотознімок заявниці та її чоловіка під час перебування на курорті.

Заявниця звернулася до суду з метою дістати заборону на оприлюднення фотографії, однак отримала відмову, яка і стала підставою для звернення до ЄСПЛ. Перед Судом заявниця стверджувала, що фотографія стосується виняткового її приватного життя (проведення часу під час відпочинку), а отже її оприлюднення становить непропорційне втручання в гарантоване ст. 8 Конвенції право на повагу до приватного життя.

Рішення ЄСПЛ. Суд встановив, що стаття, яку супроводжувала фотографія заявниці, стосувалася стану здоров'я князя Монако, а отже порушувала і питання того, як його діти проводили свій час, коли він хворіє. Це питання, безумовно, було **предметом публічного інтересу**. Фотографії, з приводу оприлюднення якої скаржилася заявниця, безпосередньо стосувалася того, про що мова йшла в статті. Отже, якщо розглядати фотографії в загальному контексті статті, то їх оприлюднення також робило певний внесок у висвітлення питання загального інтересу. У зв'язку з цим Суд звернув увагу на рішення національних судів, які чітко проводили межу між цією ситуацією та ситуацією, коли стаття використовується як формальний привід для публікації фотографій, однак не порушує питання публічного інтересу (що по суті розглядається як неправомірне втручання в право особи на повагу до приватності). Суд також звернув увагу, що хоча заявниця не виконувала ніяких функцій, однак була, безумовно, **публічною та широковідомою особою**. Суд також заявив, що заявниця не стверджувала перед національними судами про те, що фото зроблено таємно, із застосуванням засобів таємного спостереження чи в несприятливій для неї обставі, чи не відповідало дійсності. Тому не було потреби досліджувати ці питання окремо. Суд також зауважив, що фото не мало образливого характеру.

Тому Суд дійшов висновку, що національні суди дотримали балансу між правами заявниці на захист приватного життя та правом видавництва на свободу висловлювання поглядів. Отже, Суд не знайшов порушення ст. 8 Конвенції.

Приклад 2. Рішення ЄСПЛ у справі «Axel Springer AG v. Germany»[29]

Фабула справи. Газета «Більд» опублікувала статтю про деталі затримання кінозірки, відомої за головною роллю офіцера поліції в одному з популярних серіалів, за зберігання невеликої кількості кокаїну. Заголовок та вступ вказаної статті були розміщені на титульній сторінці, а продовження – всередині газети. Стаття супроводжувалася трьома фотографіями актора та гучними заголовками. Відразу після цього актор дістав судову заборону на публікацію вказаних матеріалів. У подальшому редакцію газети притягнуто до відповідальності за публікацію вказаного матеріалу. Через деякий час газета оприлюднила ще одну статтю про засудження вказаного актора у зв'язку з тими ж подіями. Суди заборонили поширення вказаного матеріалу та повторно притягнули редакцію до відповідальності. У зв'язку з цими двома національними провадженнями редакція журналу звернулася до Суду зі скаргою на порушення її прав, гарантованих ст. 10 Конвенції.

29 Axel Springer AG v. Germany, заява № 39954/08.

Рішення ЄСПЛ. Розглядаючи справу, Суд зазначив, що громадськість завжди зацікавлена в отриманні інформації щодо розслідування злочинів. Таке зацікавлення значною мірою, звісно, залежить від відомості/публічності особи, обставин її справи та перебігу провадження. Суд звернув увагу на те, що актор, про якого була стаття, знімався в популярному телесеріалі, тому був однозначно публічною особою. Він був відомий переважно за однією з ролей, а саме офіцера поліції в популярному телесеріалі. Це, на думку Суду, створювало певний зв'язок між популярністю актора та його основним персонажем. Тому той факт, що актор, який виконує роль борця зі злочинністю в телесеріалі, скоїв злочин у реальному житті, підвищує публічний інтерес до отримання такої інформації. Суд звернув увагу також на поведінку актора, а саме на те, що до описаних подій він активно шукав уваги громадськості та неодноразово розкривав деталі свого приватного життя в ході різних інтерв'ю. Це, своєю чергою, знижувало потенційний рівень захисту його приватного життя. Інформація щодо арешту була отримана від місцевої прокуратури, а тому перевірена. Ба більше, після виходу статті викладену в ній інформацію прокуратура підтвердила іншим журналам. Суд також взяв до уваги, що інформація, викладена в статтях, не містила деталей щодо приватного життя (лише щодо подій після арешту), голословних чи образливих висловлювань. Не було також фактів щодо якихось негативних для заявника наслідків від публікації статті. Щодо санкції, застосованої до компанії заявника (1000 євро), Суд зазначив, що хоч вона і не була великою, однак могла мати «охолодний ефект» на видавця, а тому не була обґрунтованою. Отже, ЄСПЛ констатував порушення ст. 10 Конвенції.

У матеріалах, розміщених в українських ЗМІ, не складно виявити випадки, які, навіть якщо не вдаватись у детальний аналіз, містять ознаки потенційного порушення права на повагу до приватного життя.

Приклад 1

На інтернет-сайті однієї з місцевих газет була висвітлена інформація про одного з ріелторів, щодо діяльності якого надходило безліч скарг від місцевих жителів. Інформація була викладена у вигляді короткої вступної статті та великої кількості відгуків жителів міста. У вступній статті, серед іншого, висвітлили адресу вказаного ріелтора.

Загалом висвітлення цієї інформації було актуальним та вагомим питанням для жителів міста. Однак розкриття адреси проживання вказаного ріелтора було надмірне і не обумовлювалося жодним інтересом, бо, не підсилюючи вагомості та значення викладених матеріалів, могло становити загрозу його життю / здоров'ю / майну.

Приклад 2

У місцевій газеті в кримінальній рубриці була оприлюднена інформація про те, що молодий хлопець внаслідок конфлікту з матір'ю скоїв самогубство. При цьому висвітлювалися особисті дані матері та небіжчика. Суспільна вагомість такої інформації дуже незначна, натомість втручання в особисте життя матері непомірно велике.

Отже, усі вказані вище публікації становлять порушення законодавства про захист персональних даних.

Що стосується *архівної інформації репресивних органів*, то обробку такої інформації, через її специфіку, окремо регламентує Закон України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917–1991 років».

2.3. Поняття «знеособлення персональних даних»

Під знеособленням персональних даних розуміється вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу.

Знеособлення персональних даних може бути особливо корисним для проведення статистичних чи наукових досліджень, коли необхідно опрацювати значні масиви часто чутливих даних, не створюючи при цьому ризику втручання в права суб'єктів персональних даних.

«Знеособлення» персональних даних слід відрізняти від так званого «псевдознеособлення» або «псевдонімізації», про яке йдеться в Загальному регламенті (*pseudonymisation*). В українській версії Регламенту[30] цей термін досить творчо перекладено як «використання псевдонімів». «Псевдонімізація» згідно з Регламентом означає обробку персональних даних таким способом, що їх більше не можна віднести до конкретного суб'єкта даних без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо і щодо неї вжито технічних та організаційних заходів, покликаних забезпечити, щоб персональні дані було неможливо віднести до фізичної особи, яку ідентифіковано чи можна ідентифікувати.

30 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.).

Отже, у разі псевдонімізації у володільця зберігається можливість за необхідності встановити, якої ідентифікованої (чи такої, що може бути ідентифікована) фізичної особи стосується та чи інша інформація. У разі знеособлення такої можливості у володільця більше немає.

Загалом же псевдонімізація – один з ефективних засобів захисту персональних даних організаційного характеру, покликаних зменшити коло осіб, які володіють доступом до персональних даних, які обробляються. Тому видається доцільним ввести вказане означення в текст Закону і так дати поштовх його частішому використанню.

Приклад. Лікарня створює реєстр пацієнтів і обробляє лише особисті дані (ім'я, прізвище, по батькові, адресу, телефон). Даним кожного пацієнта присвоюють певний ідентифікатор. З медичних документів кожного з внесених до реєстру пацієнтів видаляють (ретушують) особисті дані та проставляють ідентифікатор, після чого документи відправляють в архів. Так лише той, хто має доступ до реєстру, знатиме, кому належить відповідна медична документація. Той, хто працюватиме з медичними документами (науковець, студент, службовець управління охорони здоров'я), не зможе ідентифікувати особу, бо працюватиме зі знеособленими даними.

2.4. Поняття «володілець персональних даних»

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

Тому володільцем може бути:

- той, хто визначає мету обробки, склад даних і процедури обробки;
- суб'єкт, визначений **законом**.

Вказане означення узгоджується з положеннями ключових міжнародних документів.

За Конвенцією №108+, володілець («контролер файлу», згідно з перекладом наявним на вебсайті ВРУ) – це фізична або юридична особа, державний орган, установа чи будь-яка інша установа, що уповноважена відповідно до національного законодавства вирішувати, якою повинна бути **мета** файлу даних

для автоматизованої обробки, **які категорії** персональних даних повинні зберігатися та **які операції** повинні виконуватися з ними[31].

Регламентом надається адаптованіше до сучасних умов означення. Згідно зі ст. 4 Регламенту «володілець» означає фізичну чи юридичну особу, орган публічної влади, агентство чи іншу установу, яка самостійно чи спільно з іншими визначає **мету** та **спосіб** обробки персональних даних; якщо мета та спосіб такої обробки визначаються законодавством Союзу чи держави-члена, володілець або спеціальні критерії його призначення можуть бути передбачені законодавством Союзу чи держави-члена.

Виходячи з вказаних означень, не викликає труднощів встановити володільця, коли мова йде **про приватних суб'єктів**, які здебільшого дійсно самостійно визначають мету обробки, склад даних і процедури їх обробки. Дещо інша ситуація, коли йдеться про обробку персональних даних, наприклад ведення реєстру, **державними органами влади**. У таких випадках мета обробки, склад даних, порядок їх обробки, як і те, хто володілець, часто визначено **законами**, а ще частіше – **підзаконними нормативно-правовими актами**, а не самим володільцем.

Приклад 1. Визначення володільця законом

Згідно з п. 1 ч. 1 ст. 12-1 Закону України «Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування» Реєстр застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування «формує та веде Пенсійний фонд». Тож Пенсійний фонд України і буде володільцем цього реєстру.

Приклад 2. Визначення володільця законодавством

Згідно з Порядком функціонування електронної системи охорони здоров'я, затвердженої Постановою КМУ від 25 квітня 2018 року № 411 «володілець відомостей реєстру – уповноважений орган державної влади, який визначає мету та порядок обробки даних у відповідному реєстрі центральної бази даних». Один із реєстрів, що становить частину електронної системи охорони здоров'я, – Реєстр пацієнтів.

Порядок ведення Реєстру пацієнтів в електронній системі охорони здоров'я затверджено Наказом Міністерства охорони здоров'я України 30 листопада 2020 року № 2755. Згідно з цим порядком «володільцем

31 Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data) of 18th May, 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Date of request: 2021).

персональних даних, які містяться в Реєстрі, є Національна служба здоров'я України. Порядок обробки персональних даних, які містяться в Реєстрі, визначається володільцем персональних даних».

При цьому варто зазначити, що відступ від наданого Законом визначення щодо того, хто володілець, можливе лише у випадках, визначених «**законом**». У всіх інших випадках визначати володільця слід, виходячи з того, якими «повноваження» відносно персональних даних він володіє, зокрема чи визначає він мету обробки, склад даних та процедури обробки («повноваження володільця»).

Приклад

Згідно з ч. 1 ст. 41 Закону України «Про реабілітацію осіб з інвалідністю в Україні» «інформаційні ресурси у сфері реабілітації осіб з інвалідністю формуються у вигляді **централізованого банку даних з проблем інвалідності**, що **містить дані** [*Закон визначає склад даних. – Прим. авт.*] про реабілітаційні заклади, характер і причини інвалідності, освітній і професійний рівень осіб з інвалідністю, дітей з інвалідністю, склад сім'ї, рівень доходів, потребу і забезпечення технічними та іншими засобами реабілітації, виробами медичного призначення, реабілітаційними послугами, санаторно-курортним лікуванням, спеціальним автотранспортом тощо»[32].

Згідно з ч. 2 ст. 41 Закону «Про реабілітацію осіб з інвалідністю в Україні»: «інформаційні ресурси у сфері реабілітації осіб з інвалідністю **формуються** і **підтримуються** [*Жодне з цих повноважень не прерогатива володільця. – Прим. авт.*] в межах своїх повноважень:

на центральному рівні – центральними органами виконавчої влади, які беруть участь у здійсненні державної політики у сфері реабілітації осіб з інвалідністю;

на місцевому рівні – органами виконавчої влади Автономної Республіки Крим, відповідними підрозділами обласних, Київської та Севастопольської міських, районних, районних у містах Києві та Севастополі державних адміністрацій та органами місцевого самоврядування»[33].

32 Про реабілітацію осіб з інвалідністю в Україні : Закон України №2961-IV від 06 жовтня 2005 р. *Урядовий кур'єр*. 2005. 09 лист. (№ 213).

33 Про реабілітацію осіб з інвалідністю в Україні : Закон України № 2961-IV від 06 жовтня 2005 р. *Урядовий кур'єр*. 2005. 09 лист. (№ 213).

Згідно з п. 3 Положення про централізований банк даних з проблем інвалідності, затвердженого Постановою КМУ № 121 від 16 лютого 2011 року «Про затвердження Положення про централізований банк даних з проблем інвалідності» «**користувачами банку даних** є органи виконавчої влади, органи місцевого самоврядування, Фонд соціального захисту інвалідів, державна служба зайнятості, підприємства, що виготовляють, постачають і ремонтують технічні та інші засоби реабілітації, що призначені для безоплатного забезпечення осіб з інвалідністю, дітей з інвалідністю, інших осіб за рахунок коштів державного бюджету, та відповідають кваліфікаційним вимогам, установленим Мінсоцполітики (далі – підприємства), реабілітаційні установи, суб'єкти, що надають соціальні послуги, та інші установи, організації, що забезпечують функціонування та ведення банку даних у межах своїх повноважень»[34].

П. 6 Положення визначено повноваження кожного з користувачів банку даних центрального рівня, а п. 7 – повноваження користувачів банку даних місцевого рівня. Зазвичай повноваження зводяться до наповнення реєстру, використання наявних у ньому даних та технічного забезпечення його функціонування [*це типові функції розпорядника. – Прим. авт.*].

Згідно з п. 9 Положення передбачено, що «**держателем банку даних** є Мінсоцполітики. Держатель банку даних забезпечує **підтримку, оновлення, адміністрування, модернізацію, доопрацювання банку даних**» [*це типові функції розпорядника. – Прим. авт.*][35].

«**Адміністратором банку даних** є державне підприємство "Інформаційно-обчислювальний центр Міністерства соціальної політики України", яке здійснює заходи із супроводження програмного забезпечення банку даних, відповідає за його технічне забезпечення, збереження та захист даних банку даних, технічні та технологічні заходи з надання, блокування, анулювання доступу до банку даних на запит Фонду соціального захисту інвалідів, пошук і відбір даних для підготовки аналітичних звітів, ведення довідників банку даних» [*це типові функції розпорядника. – Прим. авт.*][36].

34 Про затвердження Положення про централізований банк даних з проблем інвалідності : Постанова Кабінету Міністрів України № 121-2011-п від 16 лютого 2011 р. *Урядовий кур'єр*. 2011. 02 бер. (№ 39).

35 Про затвердження Положення про централізований банк даних з проблем інвалідності : Постанова Кабінету Міністрів України № 121-2011-п від 16 лютого 2011 р. *Урядовий кур'єр*. 2011. 02 бер. (№ 39).

36 Про затвердження Положення про централізований банк даних з проблем інвалідності : Постанова Кабінету Міністрів України № 121-2011-п від 16 лютого 2011 р. *Урядовий кур'єр*. 2011. 02 бер. (№ 39).

Ані про володільця, ані про розпорядника не згадано жодним словом. Однак очевидно, що мету існування вказаного банку даних визначено самим Законом «Про реабілітацію осіб з інвалідністю в Україні». Згідно з частиною 4 статті 41 цього Закону «На підставі даних інформаційних ресурсів органи виконавчої влади здійснюють соціальний моніторинг, планування і прогнозування потреб осіб з інвалідністю, дітей з інвалідністю у технічних та інших засобах реабілітації, виробах медичного призначення та реабілітаційних послугах»[37].

Також згідно із Законом «Про реабілітацію осіб з інвалідністю в Україні», а саме ч. 2 прикінцевих положень, Кабінетові Міністрів України доручено протягом шести місяців з дня набрання чинності цим Законом забезпечити ухвалення нормативно-правових актів, спрямованих на реалізацію цього Закону[38]. Саме на виконання вказаного положення КМУ ухвалено Постанову № 121 від 16 лютого 2011 року «Про затвердження Положення про централізований банк даних з проблем інвалідності». Як видно вище, саме Положенням визначено, хто держатель / користувач / адміністратор, які його повноваження щодо ведення банку даних, які відомості вносять до банку даних та ін.

Тому саме КМУ і є володілець персональних даних у централізованому банку. Решта названих суб'єктів лише розпорядники – роль кожного з них у забезпеченні функціонування банку даних та обробки наявних у ньому відомостей визначена КМУ.

З цих же міркувань визначення володільця законодавством можна вважати суто «декларативним», таким, що ні до чого не зобов'язує, і виходити слід з реального стану справ. Тим більше, слід визнати, інколи положення законодавства такі заплутані з погляду понятійного апарату (див. приклад нижче), що на практиці не залишається нічого іншого, крім як самостійно визначати того, хто володілець.

Тут же варто відзначити, що передбачене Законом застереження з приводу того, що за певних умов володільця може визначати закон («фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, **якщо інше не визначено законом**»), – дослівний переклад міжнародних документів (див. вище). Однак поняття «закон», про яке йдеться в Конвенції, Регламенті та Директиві охоплює також і підзаконні нормативно-правові акти. Наприклад, ЄСПЛ застосовує автономну концепцію поняття «закон», згідно з якою, «закон» з матеріального

37 Про реабілітацію осіб з інвалідністю в Україні : Закон України №2961-IV від 06 жовтня 2005 р. *Урядовий кур'єр*. 2005. 09 лист. (№ 213).

38 Про реабілітацію осіб з інвалідністю в Україні : Закон України №2961-IV від 06 жовтня 2005 р. *Урядовий кур'єр*. 2005. 09 лист. (№ 213).

погляду охоплює писані та неписані, зокрема нижчого рангу, акти та навіть деякі документи, що ухвалили, наприклад, професійні організації, як-от Національна асоціація адвокатів України / Рада адвокатів України.

Тому слід або змінити визначення володільця в Законі, замінивши закон на законодавство, або ж припинити визначати володільця підзаконними нормативно-правовими актами. Тим більше, коли таке «визначення» володільця законодавством цілком не збігається з реальними повноваженнями такого «володільця», через що стає цілком формальним.

Приклад

Згідно з Порядком ведення реєстру хворих на туберкульоз, затвердженим наказом МОЗ № 818 від 19 жовтня 2012 року:

«– **адміністратор другого рівня** – посадова особа, яка здійснює контроль за наповненням реєстру баз персональних даних хворих на туберкульоз у межах компетенції відповідного органу державної влади, підприємства, установи, організації, певного регіону, моніторинг роботи реєстру баз персональних даних хворих на туберкульоз (далі – Реєстр) та коригування структури відомостей про хворих на туберкульоз (далі – Відомості).

– **адміністратор Реєстру** – центральний орган виконавчої влади у сфері охорони здоров'я або його структурний підрозділ, що здійснює заходи зі створення та супроводу програмного забезпечення Реєстру, збереження та захисту бази даних Реєстру, відповідає за його функціонування та надає доступ до нього;

– **база персональних даних** – іменована сукупність упорядкованих персональних даних хворих на туберкульоз в електронній формі;

– **володільці баз персональних даних** – протитуберкульозні заклади;

– **користувачі** – працівники протитуберкульозних закладів, які визначені відповідними наказами протитуберкульозних закладів відповідальними особами за ведення Реєстру та нерозголошення Відомостей, які стали їм відомі при роботі з Реєстром;

– **реєстр баз персональних даних хворих на туберкульоз** – інформаційна система збору, накопичення, обробки, оновлення, використання та поширення Відомостей, що складається з баз персональних даних;

– **розпорядник бази персональних даних** – Міністерство охорони здоров'я України»[39].

39 Про затвердження Порядку ведення реєстру хворих на туберкульоз : Наказ Міністерства охорони здоров'я України від 19.10.2012 №818. *Офіційний вісник України*. 2012. 26 лист. (№ 88). Ст. 28.

З огляду на вказані положення протитуберкульозні заклади — співволодільці реєстру. При цьому не зрозуміло, якими з повноважень володільця вони наділені.

Повноваження «розпорядника бази персональних даних» також залишаються незрозумілими, бо поняття «розпорядник» трапляється лише в означеннях. При цьому розпорядником «бази персональних даних» визначено Міністерство охорони здоров'я України (далі – МОЗ). Однак, згідно з пунктом 3 частини 1 статті 6 Закону України «Про протидію захворюванню на туберкульоз», МОЗ затверджує «порядок ведення реєстру хворих на туберкульоз та порядок обліку захворювань на туберкульоз»[40]. Саме на виконання вказаного положення МОЗ затвердило своїм наказом Порядок ведення реєстру хворих на туберкульоз, а отже фактично визначило мету обробки, склад персональних даних та порядок їх обробки. **Виходячи з цього, законом визначено, що саме МОЗ – володілець вказаної баз**и. Протитуберкульозні заклади, своєю чергою, лише дотримуються порядку, визначеного МОЗ. Їхня роль більше схожа на роль розпорядника персональних даних.

Очевидно, що законодавство України потребує подальшого вдосконалення в частині добору понятійного апарату

Загалом же при визначенні того, хто володілець, якщо, звісно, його не визначено законом, слід, як уже сказано вище, виходити з реальних повноважень того чи іншого суб'єкта.

Окрім того, слід зазначити, що залежно від наявних повноважень, як це вказано в доповненні до визначення володільця, наданого в Регламенті, володільців персональних даних може бути декілька. Очевидно, що якщо одні і ті ж дані окремо зберігаються в кількох суб'єктів (наприклад, юридичних осіб), і кожен з них наділений повноваженнями володільця, то кожен з них незалежний один від одного володілець.

Наприклад, одна компанія передає (чи продає) базу персональних даних своїх клієнтів іншій компанії. Після цього кожна з вказаних компаній незалежно одна від одної продовжують використовувати цю базу даних для власних потреб. Отже, кожна з них володілець наявних у цих базах персональних даних.

Якщо ж двоє чи більше володільців з огляду на спільні потреби створюють єдину базу персональних даних (спільно визначають мету, склад даних, порядок їх обробки), то їх слід вважати співволодільцями. Саме про це йде мова в доповненні до визначення володільця персональних даних, передбаченого

40 Про протидію захворюванню на туберкульоз : Закон України № 2586-III від 05 липня 2001 р. *Урядовий кур'єр*. 2001. 08 сер. (№ 141).

Регламентом[41]. При цьому, не важливо, чи мають вони рівний доступ до таких даних чи різний, вони залишаються їхніми співволодільцями. Такі ситуації найпоширеніші серед суб'єктів владних повноважень (див. приклад нижче).

Приклад

Спільним Наказом Адміністрації Державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 03.04.2008 № 284/287/214/150/64/175/266/75 затверджено Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон.

Вказаним положенням передбачено створення системи «Аркан». Згідно з положенням система «Аркан» – це сукупність організаційно-розпорядчих заходів, програмно-технічних і телекомунікаційних засобів, що забезпечують обробку інформації (уведення, приймання, отримання, передавання, реєстрація, зберігання) щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон України, та автоматизований доступ до інформаційних ресурсів (баз даних) суб'єктів системи «Аркан».

Ч. 5 вказаного положення систему «Аркан» визначено як міжвідомчий державний ресурс. Мету вказаної системи визначено в ч. 8 Положення («своєчасне, достовірне та функціональне повне інформаційно-аналітичне забезпечення діяльності суб'єктів системи стосовно здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або (…)»)[42].

Також вказаним документом визначено склад персональних даних (частково), які обробляє система «Аркан», види та наповнення різних підсистем, рівні доступу органів влади, що затверджували вказане положення, до відомостей у системі, порядок доступу та обміну наявною в системі інформацією, організаційні питання захисту інформації та ін.

41 Володілець – фізична чи юридична особа, орган публічної влади, агентство чи інша установа, яка самостійно чи спільно з іншими визначає мету та спосіб обробки персональних даних. *(Прим. авт.)*

42 Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон : Наказ від 03.04.2008 N 284/287/214/150/64/175/266/75. *Офіційний вісник України.* 2008. 02 черв. (№ 37). Ст. 54.

Отже, усі вказані органи влади – співволодільці персональних даних, наявних у системі «Аркан».

Разом з тим доволі поширені і ситуації, коли двоє чи більше суб'єктів частково здійснюють повноваження володільця, тобто кожен з них частково визначає мету обробки, склад персональних даних і порядок їх обробки. У такому разі кожен з них також співволоділець, однак тут є певні особливості. Якщо в попередньому випадку кожен з володільців несе відповідальність за те, як обробляють персональні дані, то в цьому разі кожен з них нестиме відповідальність лише тією мірою, якою він відповідальний за здійснення повноважень володільця.

Приклад

П. 2 ч. 1 ст. 2 Закону України «Про державні фінансові гарантії медичного обслуговування населення» передбачено створення електронної системи охорони здоров'я. Згідно з ч. 1 ст. 11 вказаного Закону порядок функціонування електронної системи охорони здоров'я затверджує Кабінет Міністрів України з урахуванням вимог законодавства про захист персональних даних[43].

Постановою Кабінету Міністрів України від 25 квітня 2018 р. № 411 затверджено Порядок функціонування електронної системи охорони здоров'я. Вказаним документом визначено загальні вимоги до обробки персональних даних в електронній системі охорони здоров'я, зокрема: мету обробки наявних у ній персональних даних (п. 23), базові стандарти їх захисту (наприклад, підпункти 9–11 пункту 8), порядок внесення відомостей у систему (п. 24), порядок верифікації наявної в системі інформації (пп. 25–29), а також реєстри, які входять до складу системи (наприклад, реєстр пацієнтів, реєстр декларацій про вибір лікаря, реєстр медичних спеціалістів (див. підпункти 1, 2 та 4 пункту 20 Порядку) та ін.)[44].

Порядком визначено, які дані вноситимуть до кожного з реєстрів. Наприклад, щодо Реєстру пацієнтів, то це унікальний номер запису в ЄДДР; РНОКПП або серія та номер паспорта; прізвище, ім'я, по батькові; дата та місце народження; адреса фактичного місця проживання або перебування; серія та номер (у разі наявності) документа, що посвідчує особу, орган, що видав документ, дата видачі, строк дії; номер телефона, адреса електронної пошти; інформація про законного представника особи (у разі наявності).

43 Про державні фінансові гарантії медичного обслуговування населення : Закон України № 2168-VIII від 19 жовтня 2017 р. *Голос України*. 2017. 30 груд. (№ 248).

44 Деякі питання електронної системи охорони здоров'я : Постанова Кабінету Міністрів України від 25 квітня 2018 р. № 411. *Урядовий кур'єр*. 2018. 25 трав. (№ 98).

Однак щодо кожного з реєстрів перелік даних не вичерпний та закінчується пунктом, де йдеться про «інші відомості, визначені МОЗ». Також підпункт 10 пункту 20 Порядку передбачено можливість створення інших реєстрів, «набір даних, у яких визначає НСЗУ. Розпорядники реєстрів та володільці їх відомостей, перелік відомостей, що вноситься до них, а також порядок їх ведення затверджуються МОЗ». Також, згідно з п. 21 Порядку особливості ведення окремих реєстрів, зокрема відомості, що вносяться до таких реєстрів, та права доступу користувачів до інформації в таких реєстрах, затверджує МОЗ[45].

На виконання вказаних положень Наказом Міністерства охорони здоров'я України від 30 листопада 2020 року № 2755 затверджено Порядок ведення Реєстру пацієнтів в електронній системі охорони здоров'я. Вказаним документом передбачено особливості ведення саме Реєстру пацієнтів. П. 10 Порядку визначено розширений список відомостей про особу, що підлягає внесенню до Реєстру. Також Порядком визначено особливості реєстрації пацієнта в реєстрі та доступу до відомостей про себе[46].

Отже, Кабінет Міністрів України та Міністерство охорони здоров'я України – співволодільці Реєстру пацієнтів, бо кожен із вказаних органів державної влади визначає окремі аспекти обробки персональних даних у реєстрі. Однак кожен з них відповідає лише за ті аспекти обробки персональних даних, які ним визначені.

Якщо на виконання підпункти 10 пункту 20 НСЗУ та МОЗ будуть створені інші реєстри, то співволодільцями наявних у них даних будуть як КМУ, так і МОЗ та НСЗУ.

Можливість спільної обробки даних допускаються і в приватному секторі, де кілька компаній можуть спільно вести бази персональних даних. Жодним положенням Закону цього не заборонено, а вказані приклади з публічного сектору це лише підтверджують. Однак у такому разі компанії повинні подбати про те, щоб належним чином розмежувати свої повноваження щодо обробки персональних даних, співволодільцями яких вони виступають. Найлогічнішим видається оформити такі відносини договором.

На завершення слід зазначити, що поняття «співволоділець» нема в українському законодавстві, однак воно існує на практиці, що підтверджується вказаними

45 Деякі питання електронної системи охорони здоров'я : Постанова Кабінету Міністрів України від 25 квітня 2018 р. № 411. *Урядовий кур'єр*. 2018. 25 трав. (№ 98).

46 Про затвердження Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я : Наказ Міністерства охорони здоров'я України від 30.11.2020 № 2755. *Офіційний вісник України*. 2021. 29 січ. (№ 7). Ст. 452.

вище ситуаціями. Як Директива, так і Регламент вже містять поняття співволодільця. У Конвенції його немає, однак воно вже внесено в Конвенцію 108+. Також у Регламенті питанню особливостей діяльності та розмежуванню повноважень співволодільців присвячено окрему статтю[47]. Тому видається доцільним врегулювати такі ситуації і в Законі України «Про захист персональних даних».

2.5. Поняття «розпорядник персональних даних»

Відповідно до ст. 2 Закону, розпорядник персональних даних – «*фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця*»[48]. У Конвенції № 108+ такого поняття, як розпорядник, немає. Зате воно наявне як у Директиві, так і в Регламенті, де розпорядник – «*це фізична чи юридична особа, орган публічної влади, агентство чи інша установа, яка обробляє персональні дані від імені володільця*»[49]. Означення в Законі практично ідентичне означенню в Директиві та Регламенті, а отже, очевидно, що воно звідти (з Директиви) і взяте.

Приклад

Підприємства, що надають житлово-комунальні послуги, укладають договори з приватними компаніями, на підставі яких останні ведуть облік щодо кількості та якості послуг, наданих підприємством споживачам, та облік виконання споживачами оплати за вказані послуги. У вказаному

47 1. Якщо два чи декілька володільців спільно визначають цілі та засоби обробки, вони співволодільці. Вони повинні на умовах прозорості встановити свої відповідні обов'язки, що відображають зміст зобов'язань за цим Регламентом, зокрема щодо реалізації прав суб'єкта даних і їхніх відповідних обов'язків щодо надання інформації, вказаної в статтях 13 і 14, шляхом досягнення домовленості між ними, за винятком, якщо і тому що, відповідні обов'язки володільців не визначено законодавством Союзу або держави-члена, дія якого поширюється на володільців. За домовленістю можна призначити координаційний центр для суб'єктів даних.
2. Домовленість, вказана в параграфі 1, повинна належним чином відображати відповідні ролі та відносини співволодільців щодо суб'єктів даних. Про сутність домовленості необхідно повідомити суб'єкта даних.
3. Незалежно від умов домовленості, вказаних у параграфі 1, суб'єкт даних може скористатися своїми правами за цим Регламентом щодо та проти кожного з володільців.

48 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

49 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.)

договорі підприємства визначають мету обробки, склад даних, повноваження компаній щодо обробки персональних даних споживачів, зобов'язання щодо їх захисту та відповідальність за порушення договору. Отже, компанії обробляють персональні дані споживачів за вказівкою підприємства та у визначених ним межах. Фактично такі компанії забезпечують технічну сторону функціонування реєстру. Тому такі компанії – класичні розпорядники.

Разом з цим схожість між Регламентом та Законом обмежується одним лише означенням.

Насамперед ст. 28 Регламенту присвячена особливостям співпраці володільця та розпорядника. Вказаним положенням передбачено низку важливих гарантій, покликаних забезпечити ефективне дотримання прав суб'єктів персональних даних. Згідно з цієї статті на володільця покладено обов'язок обирати лише таких розпорядників, які здатні забезпечити обробку персональних даних строго відповідно до положень Регламенту. Розпорядник може призначати суброзпорядника лише за згодою володільця. Взаємовідносини між володільцем і розпорядником регулюються письмовим (чи в електронній формі) договором або законом, які повинні визначати природу, характер та мету обробки персональних даних, тривалість обробки, склад даних, категорії суб'єктів персональних даних та права і обов'язки володільця тощо. Ба більше, в разі якщо розпорядник доручає обробку отриманих від володільця персональних даних іншому розпорядникові (суброзпорядникові), умови такого доручення повинні бути такими ж, як і ті, що передбачені в договорі між володільцем і розпорядником. І в разі, якщо такий суброзпорядник порушує свої обов'язки з захисту персональних даних, саме розпорядник нестиме за це відповідальність перед володільцем. Крім цього, ст. 28 Регламенту передбачено, що якщо розпорядник змінює мету обробки отриманих від володільця персональних даних чи порядок їх обробки, то в цій частині операцій з обробки саме він буде розглядатися як володілець персональних даних, а отже нестиме повну відповідальність за їх обробку[50].

Відповідно до ст. 4 Закону України «Про захист персональних даних», розпорядником персональних даних, володілець яких – 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

50 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення 23.05.2021 р.)

обробку персональних даних розпорядникові персональних даних відповідно до договору, укладеного в письмовій формі. Розпорядник персональних даних може обробляти персональні дані лише з метою і обсягом, визначеним у договорі[51].

Отже, різниця між тими гарантіями, що передбачені Законом та Регламентом, очевидна. Регламент забезпечує набагато вищий рівень захисту персональних даних. Закон, своєю чергою, залишає більшість питань щодо організації співробітництва між володільцем та розпорядником на їхній же розсуд і добросовісність. Разом з тим жодне положення Закону не перешкоджає організовувати співпрацю володільця та розпорядника(-ів) таким же чином, як це передбачено Регламентом. Ба більше володілець, який передусім несе відповідальність за дотримання Закону України «Про захист персональних даних в ході обробки», повинен бути найбільше зацікавленим у цьому. Організувавши належним чином роботу та розподіл обов'язків між ним та розпорядником, володілець зможе, з одного боку, забезпечити належний захист персональних даних, а з іншого – застрахувати себе від притягнення до відповідальності в разі скоєння тих чи інших порушень розпорядником чи суброзпорядником.

Тут слід звернути увагу на низку недоліків у вказаних положеннях Закону. Наприклад, згідно з Законом, якщо володілець персональних даних – орган державної влади чи орган місцевого самоврядування, то розпорядником може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу. Які переваги такого підприємства перед приватним підприємством не зрозуміло. Ніщо не заважає володільцеві обрати такого приватного розпорядника, який забезпечуватиме захист інформації на рівні не нижчому, аніж будь-яке державне підприємство. Звісно, що за певних умов персональні дані слід зберігати під прискіпливішим контролем з боку органів влади. Ба більше, ключові для держави реєстри, як це і відбувається на практиці, повинні вести самі ж органи влади. Однак, не виключено, що за певних умов це завдання, хоча б частково, можна передоручити приватним суб'єктам. Тож, видається, що вказане положення варто зробити гнучкішим.

Також варто переглянути означення розпорядника в Законі на предмет того, щоб (як це вище аналізувалося в контексті володільця) замінити слово «законом» на «законодавством»[52]. Ба більше, так воно і є на практиці. Зокрема, вище в розділі щодо володільця персональних даних аналізувалося декілька прикладів з ведення різних публічних реєстрів та баз даних. У всіх вказаних прикладах саме законодавством прямо визначався розпорядник персональних даних.

Також доцільним було б перейняти з Регламенту вимоги щодо форми договору (ч. 9 ст. 28 Регламенту), а саме доповнити письмову форму електронною.

---

51 Про захист персональних даних : Закон України від 23.04.2021 р. №2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

52 Розпорядник – це фізична чи юридична особа, якій володілець персональних даних або закон надав право обробляти ці дані від імені володільця. *(Прим. авт.)*

2.6. Поняття «треті особи», «одержувач» та «Уповноважений ВРУ з прав людини»

Відповідно до Закону одержувач персональних даних – це «фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа»; третя особа – це будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого ВРУ з прав людини, якій володілець чи розпорядник персональних даних передає персональні дані»[53].

Як видно із вказаних означень, поняття одержувача ширше та містить поняття третьої особи. Ключова відмінність у тому, що третя особа – окремий від володільця персональних даних суб'єкт. Передача персональних даних третій особі потребує наявності однієї з правових підстав, передбачених статтею 11 Закону (див. нижче). Одержувачем можуть бути як треті особи, так і, наприклад, працівники володільця, структурні підрозділи, яким володілець може надати право доступу до персональних даних, які він обробляє[54].

Однак за певних умов і передача персональних даних одним працівником володільця іншому може розглядатися як передача (поширення) персональних даних третій особі. Наприклад, якщо володілець чітко розмежував серед своїх працівників рівні доступу до персональних даних у базі даних, і працівник, що має такий доступ, передає персональні дані працівникові, який такого доступу не має, така дія розглядатиметься як передача персональних даних третій особі. При цьому така дія буде незаконна.

Відповідно до частини першої ст. 4 Закону до складу суб'єктів, пов'язаних із відносинами щодо персональних даних, належить також Уповноважений ВРУ з прав людини, як орган, що веде контроль за додержанням законодавства про захист персональних даних[55]. Детальніше про Уповноваженого Верховної Ради України з прав людини та його повноваження у цій сфері йтиметься нижче.

Також слід зазначити, що ст. 2 Закону містить поняття «база персональних даних», якого нема в жодному іншому положенні Закону. За таких умов варто розглянути можливість видалити вказане поняття з вказаного положення Закону[56].

---

53 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

54 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

55 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

56 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

3. ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Поняття та зміст принципів обробки персональних даних

Обробка персональних даних ґрунтується на низці принципів, які визначають основні правові засади її проведення. Вказані принципи викладено у ст. 5 Конвенції, ст. 6 Директиви, ст. 5 Регламенту та ст. 6 Закону. Фактично під принципами розуміються правила, що їх повинен дотримуватися (за незначними винятками, про які йтиметься нижче) будь-який володілець у ході виконання будь-якої обробки, на яку поширюються вказані документи. В узагальненому вигляді вказані принципи можна викласти так:

- законність і справедливість (англ. *fairness*, станом на сьогодні цей принцип частіше формулюється як *принцип прозорості обробки персональних даних*);
- легітимної мети;
- пропорційність до персональних даних до легітимної мети;
- точність (вірогідність), актуальність персональних даних;
- обробка персональних даних у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, для яких їх збирали або надалі обробляли.

Ч. 2 ст. 5 Регламенту до вказаних принципів додається також принцип ***підзвітності***. Згідно з ним кожен володілець завжди повинен бути здатним продемонструвати дотримання вказаних принципів на практиці. Також ч. 1 ст. 5 Регламенту передбачено принцип, відповідно до якого персональні дані треба обробляти способом, що забезпечує достатній рівень їх захисту[57].

Інші положення вищезазначених документів – логічне продовження, розвиток та деталізація вказаних принципів і повинні тлумачитися у їх світлі. Наприклад, положення щодо інформування суб'єкта про обробку персональних даних (ст. 12 Закону), його права отримувати інформацію про те, чи обробляються його персональні дані, хто обробляє, який порядок обробки (стаття 8 Закону) – деталізація

57 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.).

принципу справедливості обробки. Право суб'єкта вносити зміни до змісту персональних даних, які обробляє володілець, зокрема в разі їх неактуальності (стаття 8 Закону), та порядок його реалізації – своєю чергою, втілення принципу точності та актуальності. Положення щодо підстав обробки (ст. 11 Закону[58] та ст. 5 Конвенції) – розширений виклад принципу законності і т. д.

3.2. Принцип законності обробки персональних даних

Вказаний принцип закріплено в пункті а) ч. 1 ст. 5 Конвенції, пункті а) ч. 1 ст. 6 Директиви, ч. 1 ст. 6 Регламенту, а також ч. 5 ст. 6 Закону.

Вказаний принцип полягає в тому, що обробка персональних даних може проводитися лише за наявності однієї з передбачених законом підстав такої обробки. Згідно з ч. 5 ст. 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». Отже, якщо нема згоди суб'єкта, лише закон може дозволити обробку персональних даних. Разом з тим одного лиш закону, який дозволяє обробку персональних даних, чи згоди на таку обробку недостатньо для дотримання принципу законності.

Закон повинен не лише санкціонувати право збирати дані, а й встановлювати достатньо детальні правила їх обробки. У цій частині принцип законності детально роз'яснено в практиці ЄСПЛ. Відповідно до ст. 8 Конвенції втручання в гарантовані нею права (йдеться про право на повагу до приватного життя, що, як зазначено вище, охоплює право на захист персональних даних) можливе лише за умови, коли це робиться «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. Вимога щодо доступності зазвичай виконується, якщо той чи інший нормативно-правовий акт був оприлюднений. Щодо вимоги передбачуваності, то Суд встановив, що норма «передбачувана», якщо вона **сформульована з чіткістю, достатньою для того, щоб особа мала змогу, користуючись у разі потреби відповідною допомогою, регулювати свою поведінку** (див. рішення у справі «Ротару проти Румунії», заява № 27798/95, п. 48–49).

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

1) базуватися на положеннях законодавства;

2) а останнє повинне відповідати критеріям передбачуваності.

58 Про захист персональних даних : Закон України від 23.04.2021 р. №2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Класичний приклад щодо цього – рішення ЄСПЛ у справі «Ротару проти Румунії».

У справі «Ротару проти Румунії» («**Rotaru v. Romania**»)[59] Служба розвідки Румунії (далі – СР) володіла файлом, що містив персональні дані заявника (інформацію про навчання, громадську активність, публікації, участь у політичних організаціях тощо). Заявник стверджував, що зберігання вказаної інформації СР було незаконне. Суд вказав, що єдиною підставою для такого накопичення була норма в законі про СР, згідно з якою та мала право збирати, зберігати та використовувати інформацію, що має значення для національної безпеки. Суд зазначив, що жоден закон не визначав межі реалізації вказаних повноважень. Законодавство не передбачало того, *яка інформація може зберігатися, категорій осіб, щодо яких вона може збиратися, обставин, за настання яких, може відбуватися такий збір інформації, процедури збору, строків зберігання такої інформації, хто має доступ до файлів, як вони можуть використовуватися та який характер цих файлів*. Суд також зазначив, що зберігання та використання такої інформації не супроводжувалося відповідними гарантіями від зловживань, зокрема *не було незалежного контролю* (наприклад, судового) за діяльністю СР в цій частині. З огляду на зазначені факти, Суд вказав, що законодавство, яке регламентувало втручання в права заявника (обробка СР його персональних даних), не було достатньо передбачуваним. Отже, втручання в права заявника не було *законним* і порушувало статтю 8 Конвенції.

Те ж правило фактично застосовується і до обробки персональних даних на підставі згоди. Одної лише формальної згоди на обробку персональних даних недостатньо. Надаючи згоду, особа повинна розуміти, як надалі оброблятимуть її персональні дані. Однак, детальніше умови надання згоди будуть проаналізовані нижче, у розділі щодо підстав обробки персональних даних.

3.3. Принцип визначеності мети

Згідно з ч. 1 ст. 6 Закону мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних. Згідно з ч. 5 ст. 6 Закону «обробка персональних даних здійснюється для **конкретних**

59 *«Rotaru v. Romania»*, заява № 28341/95.

і **законних** цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством»[60]. Вказані положення закону – результат імплементації п. b) ч. 1 ст. 5 Конвенції №108+ («Якість даних»), відповідно до якого персональні дані, що піддаються автоматизованій обробці, повинні зберігатися для **чітких** та **легітимних** цілей і не використовуватися способом, що суперечить цим цілям[61].

Конкретність формулювання – основний крок для гарантування законності обробки. Будь-яка дія щодо персональних даних повинна відповідати визначеній меті їх обробки. Тому саме мета закладає базові межі обробки, необхідні для того, щоб надати суб'єктові персональних даних картину того, як оброблятимуться дані, а отже і можливість контролювати їх обробку. Лише знаючи, для чого потрібно обробляти його персональні дані, суб'єкт матиме розуміння того, які з його персональних оброблятимуться, впродовж якого часу, чи дійсно необхідною буде обробка цих даних тощо., а отже дістане можливість відстоювати свої права у зв'язку з обробкою персональних даних.

Приклад

Згідно з ч. 1 ст. 41 Закону України «Про реабілітацію осіб з інвалідністю в Україні» «інформаційні ресурси у сфері реабілітації осіб з інвалідністю формуються у вигляді **централізованого банку даних з проблем інвалідності**, що **містить дані** про реабілітаційні заклади, характер і причини інвалідності, освітній і професійний рівень осіб з інвалідністю, дітей з інвалідністю, склад сім'ї, рівень доходів, потребу і забезпечення технічними та іншими засобами реабілітації, виробами медичного призначення, реабілітаційними послугами, санаторно-курортним лікуванням, спеціальним автотранспортом тощо».

Згідно з ч. 4 ст. 41 цього Закону «На підставі даних інформаційних ресурсів органи виконавчої влади здійснюють соціальний моніторинг, планування і прогнозування потреб осіб з інвалідністю, дітей з інвалідністю у технічних та інших засобах реабілітації, виробах медичного призначення та реабілітаційних послугах».

Тому, якщо ч. 1 ст. 42 вказаного Закону передбачено створення **централізованого банку даних з проблем інвалідності, то ч. 4** передбачено мету обробки наявних у ньому персональних даних: «соціальний

60 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122)

61 Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data) of 18th May, 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Date of request: 2021).

моніторинг, планування і прогнозування потреб осіб з інвалідністю, дітей з інвалідністю у технічних та інших засобах реабілітації, виробах медичного призначення та реабілітаційних послугах» [62].

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

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

Метою обробки персональних даних не може бути сам факт обробки. Часто трапляються ситуації, коли як мета вказується «необхідність ведення обліку», «накопичення якомога більшої кількості інформації» тощо. У такому разі створюються ситуація, коли облік (який, власне, ніщо інше як обробка персональних даних) ведеться заради обліку (див. приклад).

Приклад

У справі **«M. K. v. France»**[63] заявника затримали за крадіжку та взяли в нього відбитки пальців. У подальшому справу закрили. Заявник звернувся до прокурора з вимогою видалити відбитки пальців, однак йому відмовили. Суди залишили без змін рішення прокурора з огляду на необхідність *накопичення якомога більшої кількості зразків для порівняння,* щоб полегшити розслідування. Суд вказав, що цілі обробки відбитків пальців у базі даних, вказані судами, були такі широкі, що фактично санкціонували збирання відбитків усього населення, що було очевидно непропорційно. Отже, держава, на думку Суду, вийшла за межі наданої їй свободи розсуду і не збалансувала інтересів особи з суспільними та порушила статтю 8 Конвенції.

Згідно з ч. 1 ст. 6 Закону в разі зміни визначеної мети обробки персональних даних на нову мету, яка **несумісна** з попередньою, для подальшої обробки даних володілець персональних даних повинен дістати згоду суб'єкта персональних

62 Про реабілітацію осіб з інвалідністю в Україні : Закон України № 2961-IV від 06 жовтня 2005 р. *Урядовий кур'єр*. 2005. 09 лист. (№ 213).

63 *«M.K. v. France»*, 19522/09.

даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом. Якщо аналізувати вказані положення Закону з урахуванням міжнародних документів, про які мова йшла вище, то видається логічним, що як ***сумісні*** в сенсі ч. 1 ст. 6 Закону слід розглядати наукові, історичні та статистичні цілі. **Тому, подальша обробка зібраних до того персональних даних для історичних, статистичних чи наукових цілей не потребує наявності окремої підстави**. Однак це можливо за умови «забезпечення їх належного захисту» (ч. 8 ст. 8 Закону)[64]/ за умови «наявності достатніх гарантій» (ст. 6 Директиви[65], Рекомендації РЄ[66]).

Такими гарантіями може виступати, наприклад, знеособлення персональних даних чи їх «псевдонімізація». Мова про вказані інструменти велася вище, у розділі 2.

Також і мета обробки персональних даних повинна бути **легітимною**, а отже не суперечити чинному законодавству держави.

3.4. Принципи адекватності, відповідності та ненадмірності

Відповідно до вказаного принципу склад та зміст персональних даних, що їх обробляє володілець, повинні відповідати легітимній меті їх обробки, бути відповідними, адекватними та ненадмірними щодо такої мети. Тобто, **по-перше**, оброблятися повинні лише ті дані, обробка яких необхідна для досягнення мети (див. Приклад 1), **по-друге**, навіть якщо певні дані і використовуються для досягнення мети, їх обробка не відповідатиме Законові, якщо її можна досягти і не проводячи обробки вказаних даних (див. приклад 2) і, **по-третє**, як це передбачено п. 2 ч. 1 ст. 6 Закону, обробка повинна відбуватися із застосуванням **засобів та способом**, що відповідають визначеним цілям такої обробки. Отже, не лише склад даних, а й спосіб їх обробки повинен відповідати критерієві пропорційності. Ба більше, принцип пропорційності повинен охоплювати весь процес будь-якої обробки персональних даних. Як зазначено вище, обробка персональних даних повинна відбуватися не довше, ніж це необхідно для законних цілей, для яких їх збирали або надалі обробляли. Також рівень організаційно-технічного захисту персональних даних повинен бути

64 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

65 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 URL: http://zakon4.rada.gov.ua/laws/show/994_242 (Дата звернення: 30.04.2021).

66 Див: Рекомендація КМ РЄ № R (97) 5 щодо захисту персональних даних, які збираються та обробляються для цілей статистики; Рекомендація КМ РЄ № R (97) 18 щодо захисту медичних даних. *(Прим. авт.)*

пропорційним до характеру та обсягу персональних даних, що обробляються. Хоч це і не пряма вимога Закону, у всіх міжнародних документах йдеться про те, що заходи захисту персональних даних повинні бути «відповідними» (англ. *appropriate*) згідно зі ст. 32 Регламенту та ст. 7 Конвенції)[67].

Приклад 1

Справа «L. H. v. LATVIA»[68]

1997 року заявниці довелося терміново робити кесарів розтин. У ході операції хірург без згоди на те заявниці провів стерилізацію. Інспекція, що вела контроль за якістю надання медичної допомоги, провела перевірку щодо цього інциденту. З цією метою вона зібрала відомості щодо надання заявниці медичної допомоги з 1996 по 2003 роки.

Заявниця оскаржила факт збору чутливої інформації щодо неї інспекцією, однак суди відмовили в задоволенні її позову.

Досліджуючи питання необхідності збору інформації щодо заявниці, Суд, серед іншого, звернув увагу на те, що інспекція зібрала непропорційно великий обсяг інформації (за період тривалістю сім років (за рік до операції та 6 після) з 3-х установ), щоб оцінити одне хірургічне втручання в 1997 році. Цьому не надано жодного обґрунтування. Тому Суд констатував непропорційність втручання в права заявниці, гарантовані статтею 8 Конвенції.

Приклад 2

МОЗ через Департамент охорони здоров'я ОДА (далі – Департамент) звернувся до лікарні з вимогою направити копії обмінних карт вагітних з результатами допологових обстежень у всіх випадках народження дітей із синдромом Дауна. Вказані документи були направлені. Згідно із запитом вказані документи запитувалися з метою проведення дослідження, необхідного для удосконалення пренатальної діагностики медичними закладами. У подальшому їх направлено вказаному дослідникові.

Вказане наукове дослідження мав проводити дослідник, тому направлення копій документів, що містять чутливу інформацію про стан здоров'я, Департаментові / МОЗ, а не безпосередньо дослідникові, не було необхідним заходом.

67 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.); Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 р. *Голос України*. 2001. 10 січ. (№ 3).

68 *«L. H. v. Latvia»*, заява № 52019/07.

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

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

Навіть якщо особа надала згоду на обробку її персональних даних, які за своєю суттю не необхідні для досягнення мети обробки, така обробка суперечитиме Законові. У зв'язку з цим неприйнятні є ситуації, коли в особи береться **«необмежена згода на обробку персональних даних»** та **«безвідклична згода»**. Чітко сформульована мета повинна надати володільцеві можливість з високим ступенем імовірності передбачити обсяг персональних даних, необхідних для її досягнення.

Якщо обробка персональних даних проводиться з метою виконання повноважень державного органу (детальніше про законні підстави обробки див. розділ 3), оброблятися повинні лише ті персональні дані, які необхідні для належного виконання цих повноважень. З огляду на те, що обробка в таких випадках ведеться на підставі закону та в порядку, визначеному законодавством, саме нормативно-правовими актами повинен визначатися склад даних, який би був пропорційним до мети їх обробки, та спосіб відповідної обробки. Тому пропорційність обробки повинна закладатися в нормативно-правовий акт уже на етапі проєкту. Роз'яснення того, чому проєкт нормативно-правового акта передбачає певний склад персональних даних, що оброблятиметься, певний строк, спосіб обробки тощо, повинно бути викладене в супровідній пояснювальній документації до законопроєкту. А що не завжди можливо передбачити оптимальний склад даних, необхідних для виконання повноважень державного органу, то законодавство повинно надавати певну дискрецію державному органові, **щоб враховувати індивідуальну ситуацію суб'єкта персональних даних. Наприклад, щоб у разі надходження звернення від такого суб'єкта щодо припинення обробки, зміни чи виправлення його персональних даних мати можливість вжити відповідних заходів.** Це узгоджуватиметься з вимогами ст. 8 Закону, якою передбачено, серед іншого, право заперечувати проти обробки, право вимагати виправлення власних персональних даних тощо.

Приклад

Справа «Gardel v. France»[69]

У Франції ухвалено закон про створення Єдиного реєстру осіб, що скоїли статеві злочини. Персональні дані заявника після скоєння ним зґвалтування були внесені до вказаного реєстру. Заявник стверджував, що зберігання його персональних даних у вказаному реєстрі було непропорційним заходом. Суд наголосив, що ведення реєстру було *необхідне та пропорційне у світлі вказаної мети* та супроводжувалося відповідними гарантіями захисту від порушення прав суб'єктів, бо, крім іншого, в разі необхідності: 1) строк зберігання інформації в реєстрі міг бути переглянутий у будь-який час до його завершення (з огляду на вік особи, плин часу, зміну особистості, життєвих обставин тощо), а 2) рішення про відмову в перегляді могло бути оскаржено в суді.

Якщо обробка проводиться з метою виконання обов'язку, передбаченого законом (наприклад, надання у разі та в порядку, визначених законодавством, інформації на запити правоохоронних та податкових органів тощо), 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.

3.5. Принцип вірогідності та точності

Персональні дані, що їх обробляє володілець, повинні бути точними та вірогідними. Це зобов'язання володільця передбачає, що з його боку вживатимуться розумні заходи, спрямовані на те, щоб підтримувати персональні дані суб'єкта в актуальному стані, а суб'єктові персональних даних забезпечується право звертатися до володільця з вимогою виправити його персональні дані.

При цьому допускаються певні відступи від вказаного принципу залежно від того, про яку сферу діяльності йдеться (медична інформація, інформація щодо причетності особи до скоєння того чи іншого злочину тощо).

69 *«Gardel v. France»*, заява № 16428/05.

Приклад

Справа «Ciubotaru v. Moldova»[70]

За часів СРСР у документах, що посвідчують особу, вказувалося етнічне походження. Більшість жителів МРСР були зареєстровані як молдовани. 2002 року заявник намагався змінити відомості щодо свого етнічного походження з молдавського на румунське. Йому відмовили у зв'язку з тим, що жоден з його батьків не був зареєстрований румуном. Заявник безуспішно оскаржував вказану відмову в судах. Йому відмовили у зв'язку з тим, що він не зміг довести, що його батьки були румунського походження.

Суд вказав, що позов заявника базувався на чомусь більшому, аніж на «суб'єктивному сприйнятті власного етнічного походження». Заявник надав докази, які свідчили про наявність у нього зв'язків з румунською спільнотою, таких як ім'я, мова, емпатія та ін. Попри це, йому відмовили з цілком формальних причин. Згідно з румунським законодавством він міг змінити відомості щодо свого етнічного походження, зокрема на румунське, лише якщо один з його батьків був зареєстрований в офіційних реєстрах як такий, що належить до вказаної спільноти. З огляду на історичні реалії Республіки Молдови, така вимога, на думку ЄСПЛ, покладала непропорційний тягар доведення на заявника. У зв'язку з цим Суд констатував порушення його прав, гарантованих ст. 8 Конвенції.

3.6. Принцип справедливості обробки персональних даних (англ. *fair processing*)

Вказаний принцип закріплено як у Конвенції №108+ (п. (a) ст. 5), Директиві (ст. 6), Регламенті (ст. 5), так і в Законі, згідно з п. 2 ч. 1 ст. 6 якого, «обробка персональних даних здійснюється **відкрито і прозоро** із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки»[71].

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

70 *«Ciubotaru v. Moldova»,* заява № 27138/04.

71 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр.* 2010. 7 лип. (№ 122).

Попри різні формулювання, розуміння вказаного принципу здебільшого однакове та охоплює такі взаємопов'язані групи прав та обов'язків суб'єктів і володільців:

1) Інформування суб'єкта персональних даних щодо обробки його персональних даних. Це передбачає обов'язок володільця автоматично надавати суб'єктові певну інформацію про обробку його персональних даних. Правило деталізується в пп. 1, 2 ч. 2 ст. 8 та ч. 2 ст. 12 (див. також ст. 10–11 Директиви, ст. 13–14 Регламенту; в Конвенції № 108 окремої статті, присвяченої цьому питанню, немає, однак воно внесене в зміст Конвенції № 108+ (стаття 8)[72]. Вказані положення деталізують обсяг інформації, що надається, та момент її надання.

2) Право доступу суб'єкта персональних даних, згідно з яким він має право знати, хто та як обробляє його персональні дані, а також їх склад та зміст. Із вказаним правилом пов'язане і право суб'єкта на виправлення, видалення та блокування його персональних даних у разі порушення якогось із зазначених вище принципів (ст. 8 Конвенції № 108, ст. 12 Директиви, ст. 15–18 Регламенту, пп. 3, 4, 5 та 6 ч. 2 ст. 8, ч. 6 ст. 16, ст. 20 та 21 Закону).

3) Право суб'єкта направляти заперечення проти обробки його персональних даних з посиланням на вагомі та легітимні особисті обставини, право суб'єкта заперечити проти автоматизованого індивідуального рішення щодо нього та проти обробки персональних даних з метою проведення цільового маркетингу. Вказані права чітко викладено в Директиві (стаття 15) та Регламенті (ст. 21–22), однак у Конвенції їх нема. У Законі вказані права викладено в загальних рисах у пп. 5, 12 та 13 ч. 2 ст. 8.

4) Повідомлення наглядового органу у визначених законом випадках про обробку персональних даних та оприлюднення останнім такої інформації.

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

72 Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data) of 18th May, 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Date of request: 30.04.2021).

3.7. Принцип підзвітності

Хоча цей принцип й не передбачено окремо національним законодавством, він імпліцитно випливає з норм Закону, якщо розглядати їх у світлі вказаних міжнародних документів.

Наприклад, враховане Законом (п. 8 ч. 2 ст. 8 та ст. 23) право застосовувати засоби правового захисту та звертатися зі скаргою передбачає не лише гарантії незалежного та безстороннього розгляду скарги та ухвалення рішення, здатного виправити порушення прав суб'єкта, в разі якщо воно сталося, а й повинно гарантувати контрольному органові (Уповноваженого ВРУ з прав людини) чи судові можливість належним чином перевіряти дотримання володільцем законодавства про захист персональних даних. Це було б неможливо, якби володілець міг не зберігати інформацію щодо обробки персональних даних (чи безслідно знищити її) та в разі отримання скарги посилатися на неможливість доведення його причетності/вини в порушенні законодавства про захист персональних даних. Саме володілець повинен у разі направлення суб'єктом скарги надати докази того, що він не скоїв порушення[73].

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

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

Зазначений принцип знайшов своє втілення і в Типовому порядку обробки персональних даних, затвердженому Наказом Уповноваженого ВРУ з прав людини від 08.01.2014 року № 1/02-14 «Про затвердження документів у сфері персональних даних».

Згідно з ч. 2 п. 2.9 Типового порядку володілець **зберігає інформацію** (документи), які підтверджують надання заявникові інформації щодо того, як оброблятимуться його персональні дані протягом усього періоду їх обробки. Згідно з п. 3.11 Типового порядку володілець / розпорядник веде облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. З цією метою володілець / розпорядник **зберігає інформацію** про: 1) дату, час та джерело збирання персональних даних суб'єкта; 2) зміну персональних даних; 3) перегляд персональних даних; 4) будь-яке передання (копіювання) персональних даних суб'єкта; 5) дату та час видалення або знищення персональних даних; 6) працівника, який виконав одну з указаних операцій; 7) мету

73 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

та підстави зміни, перегляду, передання та видалення або знищення персональних даних[74].

Тому володілець та розпорядник повинні зберігати інформацію, яка необхідна для того, щоб продемонструвати дотримання ними законодавства про захист персональних даних.

3.8. Принцип ефективного захисту персональних даних

Відповідно до ч. 1 ст. 24 Закону володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних. Згідно з ч. 2 ст. 10 Закону використання персональних даних володільцем відбувається у разі створення ним умов для захисту цих даних[75].

Згідно з п. 3.2. Типового порядку володілець, розпорядник персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки[76].

Умови для належного захисту повинні створювати володілець та розпорядник до початку обробки та з розумними інтервалами переглядати.

При визначенні рівня такого захисту вони повинні враховувати: 1) характер та обсяги персональних даних, що вони обробляють, 2) можливі наслідки від втрати таких даних, їх пошкодження, знищення, модифікації чи незаконного передання третім особам; 3) доступні технології захисту даних та організаційні заходи захисту даних і вартість їх імплементації, а також 4) ймовірність реалізації потенційних ризиків.

Отже, вказаний принцип полягає в тому, що як володілець, так і розпорядник повинні вживати належних організаційних і технічних заходів, покликаних забезпечити достатній рівень захисту персональних даних, які вони обробляють, від випадкової втрати або знищення, незаконної обробки, зокрема незаконного знищення чи доступу до них.

---

74 Про затвердження документів у сфері захисту персональних даних : Наказ № 1/02-14 від 08.01.2014 р. *Баланс*. 2014, 06 бер. 2014. № 19. Ст. 5.

75 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№122).

76 Про затвердження документів у сфері захисту персональних даних : Наказ № 1/02-14 від 08.01.2014 р. *Баланс*. 2014, 06 бер. 2014. № 19. Ст. 5.

4. ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

4.1. Загальні положення щодо підстав обробки персональних даних

Як уже зазначено вище, відповідно до ч. 5 ст. 6 Закону, обробка персональних даних відбувається лише **на підставі згоди особи або закону**[77]. Це положення конкретизується ст. 11 Закону, ст. 7 Директиви та ст. 6 Регламенту. Ст. 11 Закону встановлює вичерпний перелік випадків та умов, за яких може вестися обробка персональних даних суб'єкта. Ця стаття – перший «фільтр» на шляху до законної обробки. Якщо обробка виходить за межі передбачених ст. 11 Закону випадків, її автоматично розглядають як незаконну.

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

Згідно зі ст. 11 Закону («Підстави для обробки персональних даних»): «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;

6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта

77 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

персональних даних у зв'язку з обробкою його даних переважають такі інтереси»[78].

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

Згода	Закон
1) Згода суб'єкта персональних даних на обробку його персональних даних;	1) Дозвіл на обробку персональних даних, наданий володільцеві персональних даних відповідно до закону лише для здійснення його повноважень;
2) укладення та виконання правочину, сторона якого – суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для вжиття заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних.	2) захист життєво важливих інтересів суб'єкта персональних даних;
	3) необхідність виконання обов'язку володільця персональних даних, який передбачений законом;
	4) необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес[79].

Слід зазначити, що згідно зі ст. 6 Регламенту **«необхідність захисту законних інтересів» як підставу обробки персональних даних не можуть використовувати державні органи влади** при виконанні покладених на них завдань[80]. Хоч у Законі такого правила немає, однак з ним не можна не погодитися, бо державні органи зобов'язані діяти лише на підставі, у межах повноважень та способом, що передбачені Конституцією та законами України. Інтерес

78 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

79 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

80 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.).

же суто приватноправова категорія. Також слід зазначити, що використання державними органами згоди як підстави для обробки персональних даних повинно бути зведене до мінімуму. При її використанні слід враховувати, що **суб'єкт має право в будь-який час відкликати свою згоду**, після чого обробка повинна бути негайно припинена.

Вказаний перелік підстав обробки персональних даних вичерпний.

Обробка чутливих категорій персональних даних, про які мова йшла вище, ведеться лише у випадках та на умовах, передбачених ст. 7 Закону. Критерії законної обробки чутливих даних, визначені ст. 7 Закону, **детальніші та обмеженіші проти тих, що передбачені ст. 11 Закону**, та повністю ними охоплюються. Зокрема, договір не законна підстава для обробки чутливих категорій даних, як і законний інтерес, передбачений ст. 11 Закону[81].

Виходячи з указаного вище, слід ще раз наголосити на тому, що «обробка на підставі закону» та «законність (легітимність) обробки» – різні поняття. Законність обробки – принцип, який передбачає, що вона повинна вестися 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 і відсилає до пп. 2, 4, 5 та 6 ч. 1 ст. 11 Закону[82]. Остання виступає по суті протилежністю обробки, що базується на підставі згоди.

4.2. Персональні дані та конфіденційна інформація

У національному законодавстві паралельно існують два поняття, які запроваджено Законом України «Про інформацію», а саме: «персональні дані» та «конфіденційна інформація». Якщо поняття «персональні дані» стосувалося характеру інформації (інформація про особу), то поняття «конфіденційності» характеризувало відкритість інформації та режим доступу до неї. З плином часу їх законодавчий зміст дещо змінювався. Чіткого співвідношення між указаними поняттями не було. Часто режим конфіденційної інформації, який передбачав закритість доступу до неї, поширювався на всі персональні дані, для того щоб обмежити доступ до них. Така традиція існує до цього часу, а тому співвідношення вказаних понять потребує додаткового роз'яснення.

81 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

82 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Як уже йшлося вище, згідно зі статтею 32 Конституції не допускаються 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 виходить, що інформація про особу (персональні дані) може бути як конфіденційною, так і ні.

Згідно зі статтею 11 Закону України «Про інформацію» інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Не допускаються 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 захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження[83].

Згідно зі ст. 21 вказаного Закону інформація з обмеженим доступом конфіденційна, таємна та службова інформація. Конфіденційна – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися **на бажання (за згодою) відповідної особи** у визначеному нею порядку відповідно до передбачених нею умов, а також **в інших випадках, визначених законом**[84].

Згідно з ч. 2 ст. 5 Закону «Про захист персональних даних» персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Вказаною статтею також передбачено низку категорій персональних даних, що не можуть бути віднесені до інформації з обмеженим доступом та передбачено, що «законом може бути заборонено віднесення інших відомостей, що є персональними даними, до інформації з обмеженим доступом». Також, як аналізувалося вище, згідно зі ст. 6 та 11 Закону обробка персональних даних проводиться **за згодою особи або на підставі закону**[85].

Відповідно до ч. 1 та ч. 2 ст. 6 Закону України «Про доступ до публічної інформації» інформація з обмеженим доступом – це: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація. Обмеження доступу до інформації відбувається **відповідно до закону** при дотриманні сукупності таких вимог: 1) лише в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації

83 Про інформацію : Закон України 2657-XII від 02 жовтня 1992 р. *Відомості Верховної Ради України*. 1992. 01 груд. (№ 48). Ст. 650.

84 Про інформацію : Закон України 2657-XII від 02 жовтня 1992 р. *Відомості Верховної Ради України*. 1992. 01 груд. (№ 48). Ст. 650.

85 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

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[86].

Не зовсім коректне є автоматичне віднесення всіх персональних даних до конфіденційної інформації, що передбачає «презумпцію» їх закритості.

Разом з тим, попри певні суперечності в указаних нормативно-правових актах щодо того, чи належать персональні дані до конфіденційної інформації, безперечним залишається те, що їх мають обробляти лише **за згодою особи або на підставі закону**. Вказана теза не суперечить жодному з перелічених документів.

Конкретніше підстави обробки персональних даних викладено у ст. 7 та 11 Закону. Вони, своєю чергою, також виходять з того, що для обробки персональних даних потрібна або згода суб'єкта, або закон, а отже узгоджуються з рештою положень законодавства. Попри вичерпність переліку підстав для обробки персональних даних, вони достатньо широкі для того, щоб врахувати всі можливі ситуації. Вони також узгоджуються із загальноприйнятими вимогами щодо обробки персональних даних (ідеться про Конвенцію № 108 та Регламент).

Отже, не прив'язуючись до понять конфіденційної інформації чи інформації з обмеженим доступом, при обробці персональних даних слід виходити саме з указаних положень Закону України «Про захист персональних даних».

4.3. Обробка на підставі згоди суб'єкта

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 в письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення позначки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення позначки (ст. 2 Закону)[87].

86 Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2939-VI. *Голос України*. 2011. 09 лют. (№ 24).

87 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Із зазначеного видно, що для того, щоб відповідати Законові, згода повинна володіти трьома невіддільними ознаками:

- **добровільність** – нема прямого чи опосередкованого примусу при наданні згоди. Тому як згідно з Конвенцією, Директивою, Регламентом, так і згідно із Законом (п. 11 ч. 2 ст. 8) згоду суб'єкт може відкликати в будь-який час;
- **поінформованість**: перед наданням згоди на обробку персональних даних суб'єкт повинен отримати вірогідну інформацію про те, хто, з якою метою буде обробляти його персональні дані, кому будуть передаватися, які саме дані (склад даних), а також про права, визначені Законом (ст. 12 Закону). Така інформація повинна бути надана в доступному вигляді і володілець повинен за будь-яких умов мати можливість підтвердити факт надання такої інформації суб'єктові;
- **форма** надання згоди може бути фактично будь-якою. Однозначність згоди не повинна викликати сумнівів і володілець повинен мати змогу підтвердити її наявність упродовж усього часу проведення обробки персональних даних.

Договір. Аналогічні критерії застосовуються й у разі обробки на підставі договору. Згідно зі статтею 203 Цивільного кодексу України «волевиявлення учасника правочину має бути вільним і відповідати його внутрішній волі». Укладення договору презюмує надання згоди на обробку даних, необхідних для його виконання сторонами.

4.4. Обробка персональних даних на підставі закону

Обробка персональних даних на підставі закону передбачає наявність однієї з чотирьох підстав, визначених пунктами 2, 4, 5 та 6 частини 1 статті 11 Закону:

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

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

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

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

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

Приклад 1

Статтею 7 Закону України «Про очищення влади» передбачено створення Єдиного державного реєстру осіб, щодо яких застосовано положення цього Закону [88]. Вказана стаття встановлює категорії суб'єктів, персональні дані яких міститимуться в указаному Реєстрі, порядок їх збору, склад даних, склад даних, що підлягають оприлюдненню, а також суб'єктів, яким може надаватися інформація з Реєстру тощо.

Приклад 2

Відповідно до п. 2 ч. 1 ст. 34 Закону України «Про загальнообов'язкове державне соціальне страхування на випадок безробіття» «Фонд має право (…) перевіряти достовірність відомостей, поданих роботодавцем для отримання коштів Фонду, дотримання порядку використання роботодавцем виділених йому коштів Фонду та зупиняти виплати з Фонду в разі відмови або перешкоджання з боку роботодавця у проведенні перевірки, виявлення фактів подання ним Фонду недостовірних відомостей або порушення порядку використання роботодавцем коштів Фонду»[89].

Очевидно, що реалізація вказаного права потребуватиме обробки персональних даних суб'єкта/ів персональних даних. Отже, на підставі вказаного положення, а також п. 2 ч. 1 ст. 11 цього Закону Фонд матиме право обробляти персональні дані в *межах, які необхідні для реалізації вказаного повноваження*[90].

88 Про очищення влади : Закон України № 1682-VII від 16 вересня 2014. *Голос України*. 2014. 15 жовт. (№ 198).

89 Про очищення влади : Закон України № 1682-VII від 16 вересня 2014. *Голос України*. 2014. 15 жовт. (№ 198).

90 Про очищення влади : Закон України № 1682-VII від 16 вересня 2014. *Голос України*. 2014. 15 жовт. (№ 198).

Вказана підстава основна для обробки персональних даних державними органами. Слід, однак, наголосити, що дотримання вказаного положення – лише перший крок органу державної влади чи органу місцевого самоврядування на шляху до законної обробки. Для того щоб повною мірою відповідати принципові законності, порядок обробки персональних даних такими володільцями повинен детально регламентуватися законодавством та внутрішніми документами володільця. Відповідне законодавство повинне встановлювати межі повноважень державних органів щодо обробки персональних даних. Тому за звичайних умов воно повинно бути достатньо чітким, щоб дати суб'єктам, чиї дані обробляють, розуміння того, за яких умов, які дані, впродовж якого часу та хто може обробляти, а також який порядок доступу до таких даних та їх передачі третім особам тощо.

Саме таке розуміння відповідає ч. 2 ст. 19 Конституції України, згідно з якою «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». Таке розуміння випливає і з положень Закону, зокрема принципів законності та справедливості обробки, мова про які йшла вище.

Такий підхід відповідатиме також практиці ЄСПЛ, сформованій у рішеннях «Ротару проти Румунії», «Заїченко проти України № 2», «П. Г. та Дж. Г. проти Великої Британії».

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

У рамках розгляду справи щодо скоєння заявником адміністративного правопорушення суд призначив проведення стаціонарного обстеження психічного стану здоров'я заявника з метою встановлення того, чи міг він бути притягнутим до відповідальності. А що в матеріалах справи не було матеріалів, необхідних для проведення обстеження, суд дав вказівку органам внутрішніх справ зібрати необхідну інформацію. З цією метою співробітники міліції опитали родичів, сусідів та друзів заявника, отримали довідку з лікарні щодо проходження заявником лікування. Суд констатував порушення прав заявника, бо нема спеціальних положень законодавства, що регламентували б порядок проведення примусового обстеження (і зокрема збору інформації) в рамках розгляду справи про скоєння адміністративного правопорушення[91].

91 *«Zaichenko v. Ukraine (no. 2)»*, заява № 45797/09.

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

Під час перебування у відділі поліції розмова заявників з поліціянтами була записана. Зразки їхніх голосів збережено для проведення експертизи (в ході якої їх порівнювали з іншими зразками, які належали особам, причетним до скоєння злочину). Європейський суд з прав людини зазначив, що в законодавстві Великої Британії не було норм, що регламентували б процес відбору зразків голосу в приміщенні управління поліції. Тому таке використання зразків їхніх голосів було незаконне та порушувало їхні права, гарантовані статтею 8 Конвенції[92].

Приклад 3. Справа «Avilkina v. Russia»

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

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

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

– особи, щодо яких проводили перевірку, не були підозрюваними, обвинуваченими (просто проводилася перевірка діяльності релігійної організації);
– медичні заклади не зверталися до суду з метою проведення примусового переливання (що можливо у разі загрози життю), не повідомляли про скоєння злочину чи примушування релігійною організацією своїх вірних до відмови від лікування;
– прокуратура навіть не спробувала дістати згоду пацієнтів;
– не було порядку реалізації повноважень прокуратури на отримання документів;

92 «*P. G. and J. H. v. the United Kingdom*», заява № 44787/98.

– суди переглянули скаргу заявників, однак не дослідили питання дотримання справедливого балансу між інтересами проведення перевірки та правами суб'єктів на повагу до їхнього приватного життя інтересів, не надали обґрунтування передачі інформації, тим самим підтвердивши необмежені повноваження прокуратури[93].

Б) Захист життєво важливих інтересів суб'єкта персональних даних. Як приклад, можна навести ситуацію, пов'язану з наданням невідкладної медичної допомоги. Надання медичної допомоги за будь-яких обставин передбачає необхідність обробки даних щодо стану здоров'я особи. У разі наявності ознак прямої загрози життю особи та необхідності надання невідкладної медичної допомоги за умови неможливості отримання з об'єктивних причин згоди (наприклад, через втрату свідомості) на медичне втручання від самої особи чи її законних представників, медичне втручання проводиться без такої згоди (статті 3, 37 та 43 Закону України «Основи законодавства України про охорону здоров'я»[94]). Тож і обробка необхідних для цього персональних даних ведеться без згоди особи, безпосередньо на підставі вказаного положення ст. 11 Закону.

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

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

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

93 *«Avilkina and Others v. Russia»*, заява № 1585/09.

94 Основи законодавства України про охорону здоров'я : Закон України від 19 листопада 1992 р. № 2801-XII. *Відомості Верховної Ради України.* 1993. 26 січ. (№ 4).

Приклад

Підприємство отримує ухвалу слідчого судді про тимчасовий доступ до речей і документів, що є в його розпорядженні. Виконання ухвали передбачає, серед іншого, надання персональних даних одного з працівників. Законом передбачено обов'язок суб'єктів, які отримують таку ухвалу, надавати визначену в ній інформацію. Вказані відомості необхідні для розслідування злочину в рамках порушеного кримінального провадження. У такому разі підприємство **зобов'язане** надати таку інформацію. Підставою передачі персональних буде необхідність виконання обов'язку, передбаченого законом.

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

Вказана підстава застосовується лише до роботи приватних суб'єктів. Достатньо зазначити, що як уже говорилося вище, суб'єкти, що не належать до державних органів, у своїй діяльності керуються не лише правами, визначеними законом, а й законними інтересами. Класичний приклад законного інтересу у сфері захисту персональних даних – прямий маркетинг. Прагнення просувати свої товари шляхом направлення повідомлення потенційним споживачам не право, гарантоване законом, як і не заборонене ним, а тому воно інтерес.

В Україні обробка персональних даних для цілей, наприклад, прямого маркетингу регламентується загальними положеннями Закону. Разом з тим, з огляду на масовість обробки персональних даних для вказаних цілей КМ РЄ ухвалив з цього приводу окрему рекомендацію R (85) 20 «Щодо захисту персональних даних, які використовуються для цілей прямого маркетингу».

Згідно з указаним документом володільцям загалом дозволено накопичувати персональні дані з метою проведення цільового маркетингу. Це стосується як даних, зібраних володільцем у ході власної діяльності, тобто даних його клієнтів, так і даних, отриманих з відкритих джерел. За умови дотримання гарантій, передбачених національним законодавством, та де необхідно згоди особи, допускається використання з цією метою і спеціальних категорій персональних даних.

Разом з тим рекомендацією передбачена низка додаткових гарантій, коли йдеться про передачу володільцем власної бази клієнтів іншим володільцям. Такі дії можливі лише за умови повідомлення суб'єкта про таку можливість або на етапі збору його даних, або в подальшому та коли нема заперечень суб'єкта з цього приводу. Також така передача персональних даних повинна

проводитися на підставі договору. На завершення, варто зазначити, що суб'єкт може в будь-яких момент вимагати беззастережного видалення своїх персональних даних з реєстрів, які використовуються для маркетингових цілей.

4.5. 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 і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

Разом з тим ч. 2 ст. 7 Закону, як і ст. 8 Директиви та ст. 9 Регламенту, встановлює вичерпний перелік випадків, коли дозволяється обробляти чутливі дані. Вказане відповідає і положенням ст. 6 Конвенції № 108, яка окремо виділяє чутливі категорії даних і вимагає, щоб їх обробка забезпечувалася відповідними гарантіями.

Відповідно до ч. 2 ст. 7 Закону дозволяється обробка чутливих категорій даних, якщо вона:

1) ведеться за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних.

Відмінність між цим та вказаним вище положенням статті 11 Закону в тому, що для того, щоб проводити обробку чутливих категорій даних, необхідна *однозначна* згода особи. Тлумачний словник означує слово «*однозначний*» як таке, що має тільки одне значення. Аналогічна термінологія використовується і в Директиві. Отже, мається на увазі, що надання згоди має бути таким, що не викликає жодного сумніву в її наданні.

2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту[95].

Перша і найважливіша умова для застосування вказаного положення – **наявність норми закону**, яка дозволяє збирати такі дані для цілей 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.

---

95 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Приклад такої підстави обробки чутливих категорій персональних даних – ч. 2 ст. 24 Кодексу законів про працю України (КЗПУ), відповідно до якої «при укладенні трудового договору громадянин зобов'язаний подати (…) у випадках, передбачених законодавством, – також документ (…) про стан здоров'я (…)». Наказом Міністерства внутрішніх справ України від 12.05.2016 року № 377 «Про затвердження Порядку формування та ведення особових справ поліцейських» передбачено, що особова справа поліцейського повинна містити: (…) документи про проходження медичного та психофізіологічного обстеження, перевірку рівня фізичної підготовки. Отже, п. 2 ч. 2 ст. 7 Закону в поєднанні з указаним положенням КЗПУ та наказу МВС – підстава для обробки медичної інформації про особу для цілей 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 аналог до п. 4 ч. 1 ст. 11 Закону.

4) ведеться 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 лише персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їхньої діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних.

Вказане положення дозволяє законним 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 ч. 2 ст. 7 Закону, наприклад для цілей контррозвідувальної діяльності, боротьби з тероризмом, захисту правової вимоги тощо).

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

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

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

Слід зазначити, що згідно з практикою ЄСПЛ при наданні сторонами як доказів документів, що містять персональні дані інших осіб, навіть якщо такі відомості мають певне значення для справи, не повинно автоматично тягнути за собою

їх долучення до матеріалів справи, а тим паче висвітлення в тексті рішення суду.

Приклад. Справа «L. L. v. France»

Дружина заявника розпочала судове провадження щодо розлучення. У рамках цього провадження вона надала суду як докази того, що неодноразово зазнавала фізичного насильства з боку чоловіка, численні медичні довідки. Крім цього, вона стверджувала, що причиною такої агресивної поведінки чоловіка була його алкогольна залежність. На підтвердження факту такої залежності вона надала судові свідчення двох сестер заявника та лист, направлений хірургом, який проводив операцію заявникові, терапевтові заявника. У листі йшлося про те, що заявник страждав панкреатитом «на фоні алкоголізму» та що наслідки панкреатиту можна було б усунути, лише якщо заявник припинить зловживати алкоголем. Суди задовольнили позов та виклали зміст вказаного листа в тексті рішення суду.

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

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

Суд вказав, що такі дії національного суду відповідали домашньому законодавству, згідно з яким будь-який документ, за винятком низки випадків, під які ця ситуація не підпадала, міг бути використаний як доказ. Заявникові була також надана можливість надати коментарі щодо вагомості такого доказу.

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

Разом з тим Суд зазначив, що вказаний лист був лише вторинним доказом і що тих же висновків можна було б досягнути без його використання. Тому використання вказаного листа не було необхідним та пропорційним у світлі поставленої мети його використання – «захисту прав та свобод інших осіб».

Додатково Суд вказав, що домашнє законодавство не надавало достатніх гарантій при використанні інформації приватного характеру в ході таких судових проваджень.

6) необхідна для цілей охорони здоров'я, встановлення медичного діагнозу, забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляють медичний працівник або інша особа закладу охорони здоров'я чи фізична особа – підприємець, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівники, на яких покладено обов'язки щодо забезпечення захисту персональних даних і на яких поширюється дія законодавства про лікарську таємницю, працівники центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних.

Це положення очевидне та не потребує додаткових коментарів. Певні зауваження викладено в кінці цього розділу.

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

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

Ця підстава видається очевидною, однак виникають певні запитання, пов'язані з формулюванням «стосується вироків суду». Виходячи з актуального стану справ, його слід розуміти як таке, у якому мова йде не лише про персональні дані, вказані в тексті вироку, а й про ті, що стосуються кримінального провадження загалом, однак варто сформулювати таке положення в цій частині чіткіше.

Також видається доцільним доповнити перелік поняттям адміністративних правопорушень, бо оформлення матеріалів щодо скоєння 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 у стані алкогольного, наркотичного чи іншого сп'яніння або під впливом лікарських препаратів, що знижують їхню увагу та швидкість реакції (стаття 130 КУпАП) тощо.

8) стосується даних, які явно оприлюднив суб'єкт персональних даних.

За загальним правилом, 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

вести обробку оприлюдненої інформації про особу, повинен переконатися в тому, що така особа дійсно надала згоду. Інакше обробка ним персональних даних суб'єкта буде вважатися незаконною.

У цій частині, однак, слід зробити застереження про те, що вказане положення не можна тлумачити як таке, що надає право на обробку оприлюднених персональних даних державним органам влади, якщо така обробка не передбачена їхніми повноваженнями чи іншими легітимними підставами (див. вище).

Також слід зазначити, що, виходячи з практики ЄСПЛ, підхід до обробки інформації, що є у відкритому доступу, змінюється, особливо коли йдеться про обробку володільцями значних масивів даних.

У цьому зв'язку особливо цікавими видаються висновки ЄСПЛ у його рішенні в справі *«Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC]»*[96]. У вказаній справі перший заявник публікував у журналі відомості щодо оподаткованих доходів та активів усіх платників податків, а другий – запустив послугу надання вказаної інформації щодо конкретної особи в есемес-повідомленні. Згідно з національним законодавством вказана інформація була публічна і регіональні фіскальні органи регулярно її публікували. Заявники ж збирали цю інформація в регіональних органах і поширювали її способом, указаним вище.

У подальшому вказаним компаніям заборонили публікувати цю інформацію способом, яким вони це робили. Заявники звернулися до ЄСПЛ зі скаргою за ст. 10 Конвенції.

Серед усього іншого, Суд проаналізував те, чи можна вважати, що публікація вказаних відомостей компаніями-заявницями могла становити втручання в права платників податків, гарантованих ст. 8 Конвенції. Висновки в цій частині особливо цікаві.

ЄСПЛ зазначив, що «там, де зроблено компіляцію даних щодо певної особи, обробка чи використання цих персональних даних чи публікація відповідного матеріалу способом чи мірою, які виходять за межі передбачених *(in a manner or degree beyond that normally foreseeable)*, можуть поставати питання щодо захисту права на повагу до приватного життя». Для таких ситуацій Суд вказав, що національне законодавство має містити відповідні гарантії, покликані запобігти використанню персональних даних всупереч гарантіям, передбаченим ст. 8 Конвенції.

Отже, ЄСПЛ встановив, що ст. 8 Конвенції передбачає свого роду «право на інформаційне самовизначення *(informational self-determination)*, яке дозволяє індивідам покладатися на їхнє право на приватність стосовно даних, які, хоч і нейтрального характеру, збираються, обробляються та поширюються колективно в такій формі чи таким способом, що їх права, гарантовані ст. 8, можуть бути зачеплені».

---

96 *«Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland»*, заява № 931/13, пп. 133–138.

Виходячи з вказаних висновків ЄСПЛ, використання наявних у публічному просторі відомостей про особу не необмежене. Серйозні питання щодо дотримання права на повагу до приватного життя можуть поставати у разі цілеспрямованого збору даних про особу та використання їх для цілей, що істотно відрізняються, від тих, з якими вони оприлюднювалися. Особливо гостро це питання може постати, коли накопичені так дані можуть використовуватися способом, що має якісь наслідки для суб'єкта персональних даних.

Це рішення також наблизилося до питання «профайлингу». Збір доступних публічному просторі даних про особу (і зокрема легкодоступних, наприклад, за певну плату) з метою формування її портрету / прогнозування її поведінки / купівельних спроможностей і вподобань розкриває такі відомості про особу, які вона, очевидно, не мала наміру демонструвати, викладаючи інформацію про себе в публічному просторі, і про які могла й сама не знати. Використання таких механізмів можливе лише за умови наявності відповідних гарантій захисту прав особи, зокрема права заперечити проти такого використання чи оскаржити його в наглядовому органі або суді.

•••

На завершення, слід наголосити, що в певних аспектах ст. 7 Закону містить істотні прогалини.

Виходячи з положень вказаної статті, нема законних підстав для обробки, наприклад, інформації щодо стану здоров'я для цілей соціального захисту, страхування та пенсійного забезпечення. Такий стан справ суперечить реаліям.

Приклад

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

Навіть ширше тлумачення положень цієї статті не виправляє ситуацію. Обробка для цілей «соціального захисту, страхування та пенсійного забезпечення та ін.» частково потрапляє в сферу охорони здоров'я. Тому обробка персональних даних для таких цілей могла б вестися на підставі п. 6 ч. 2 ст. 7 Закону (див. вище). Однак це положення має досить вузьке застосування, бо на вказаній підставі чутливі дані можуть обробляти лише «**медичний працівник або інша особа закладу охорони здоров'я, або фізична особа – підприємець**, яка одержала ліцензію на провадження господарської діяльності з медичної практики, **та її працівники**» та «**працівники центрального органу виконавчої влади**, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних». Працівники органів соціального захисту не потрапляють у жодну категорію. При цьому таких обмежень щодо обробки чутливих даних для цілей охорони здоров'я не має ні в Директиві[97], з якої це положення скопійовано, ні в Регламенті.

Те саме стосується низки інших аспектів. Останні події, пов'язані з глобальним поширенням вірусу COVID-19 засвідчують, що для цілей охорони громадського здоров'я та запобігання транскордонному поширенню хвороб дозвіл на обробку персональних даних медичного характеру може бути наданий набагато ширшій категорії осіб.

Поза всяким сумнівом, інколи за умови дотримання відповідних гарантій обробка спеціальних категорій персональних даних може бути необхідна для історичних, статистичних чи наукових цілей. Однак Закон не передбачає і такої можливості.

Отже, станом на сьогодні можна стверджувати про потребу в перегляді ст. 7 Закону.

Разом з тим не можна вважати всі ситуації обробки чутливих категорій персональних даних, що не охоплюються статтею 7 Закону, незаконними. Ст. 25 Закону передбачено можливість відступу, серед іншого, від положень ст. 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 тоді, коли це не передбачено статтею 7 Закону.

97 Згідно з Директивою «Держави-члени забороняють обробку персональних даних (…), що стосуються здоров'я та статевого життя. 3. Частина 1 не застосовуватиметься там, де обробка персональних даних необхідна для цілей превентивної медицини, діагностики, забезпечення догляду чи допомоги або надання медичних послуг, та ці дані обробляє спеціаліст-медик, на якого згідно з національним законодавством чи правилами, що ухвалили компетентні національні органи, поширюється зобов'язання щодо збереження професійної таємниці, чи інша особа, на яку поширюються еквівалентні зобов'язання щодо конфіденційності». *(Прим. авт.)*

Приклад. Позиція Уповноваженого ВРУ з прав людини

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

Персональні дані щодо стану здоров'я Законом віднесені до категорії так званих «чутливих» персональних даних. Статтею 7 Закону встановлено вичерпний перелік випадків щодо того, коли і хто може виконувати обробку таких персональних даних. Викладена в листі Фонду ситуація не потрапляє до вказаного переліку.

Водночас статтею 25 Закону визначено, що обмеження дії статей 6, 7 і 8 цього Закону може відбуватися у **випадках, передбачених законом**, **якою мірою це необхідно** в демократичному суспільстві **в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб**[98].

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

Законом України «Про загальнообов'язкове державне соціальне страхування» визначено, що Фонд соціального страхування України – орган, який веде (…) контроль за використанням коштів, забезпечує фінансування виплат за цими видами загальнообов'язкового державного соціального страхування (…). Згідно зі статтею 31 Закону України «Про загальнообов'язкове державне соціальне страхування» підстава для призначення допомоги за тимчасової непрацездатності – виданий у встановленому порядку листок непрацездатності[99].

98 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

99 Про загальнообов'язкове державне соціальне страхування : Закон України № 1105-XIV від 23 вересня 1999 р. *Відомості Верховної Ради України*. 1999. 26 лист. (№ 46). Ст. 403.

Відповідно до статті 9 зазначеного Закону проведення перевірки обґрунтованості видачі та продовження листків непрацездатності застрахованим особам — одне з основних завдань Фонду соціального страхування України та його робочих органів. З цією метою Фонд має право розслідування страхових випадків та обґрунтованості виплати матеріального забезпечення, страхових виплат. Відповідно до статті 10 Фонд має право перевіряти вірогідність відомостей, поданих роботодавцем для отримання коштів Фонду.

Отже, 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 – об'єктивна необхідність, бо саме ця інформація дозволяє визначити обґрунтованість видачі та продовження листків непрацездатності, які служать підставою для виплати коштів.

Отже, надання Фондові доступу до тих персональних даних особи, **які необхідні** для перевірки обґрунтованості видачі та продовження листків непрацездатності, відповідатиме вимогам Закону України «Про захист персональних даних».

Детальніше вказані питання проаналізовані в розділі, присвяченому обмеженню прав, гарантованих Законом.

5. ПРАВА СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ

5.1. Право суб'єкта на отримання інформації щодо обробки його персональних даних

Володілець персональних даних згідно із Законом зобов'язаний автоматично надавати суб'єктові певну інформацію про обробку його персональних даних.

Відповідно до ч. 2 ст. 12 Закону суб'єкта персональних даних повідомляють про: 1) володільця персональних даних, 2) склад та 3) зміст зібраних персональних даних, 4) його права, визначені Законом, 5) мету збору персональних даних та 6) осіб, яким передаються його персональні дані. Про інформацію, вказану в ст. 12 Закону, повідомляють суб'єкта 1) в момент збору персональних даних, якщо персональні дані збирають у суб'єкта персональних даних, або 2) протягом тридцяти робочих днів із дня збору персональних даних в інших випадках[100].

Це зобов'язання володільця пов'язане з правами суб'єкта персональних даних, закріпленими в ст. 8 Закону, знати про обробку його персональних даних та їх зміст.

З одного боку, воно запорука дотримання інших прав, а саме права доступу до своїх персональних даних, бо якщо суб'єкт не знає про те, що його персональні дані може обробляти конкретний володілець, у нього може не бути причин звертатися до останнього (зокрема з метою захисту своїх прав).

З іншого боку, це положення сформульоване без усяких застережень, у зв'язку з чим видається, що кожен володілець зобов'язаний повідомляти кожного суб'єкта про обробку його персональних даних. Однак така ситуація нелогічна. Важко уявити, щоб у процесі проведення оперативно-розшукової діяльності чи кримінального провадження, у ході яких збирається інформація про суб'єкта, правоохоронні органи повинні були б повідомляти його про це. Так само нелогічно, щоб суб'єкта повідомляли 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 проводиться зазвичай таємно, у другому – право збирати інформацію про особу зазвичай

100 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

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. Як стаття 10, так і 11 Директиви вказують на те, що повідомляти про порядок обробки непотрібно, якщо суб'єктові і так відома ця інформація[101]. Також є певні обмеження щодо повідомлення суб'єкта, коли інформація збирається для наукових, статистичних чи історичних цілей. Регламент містить ще детальніші винятки[102].

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

Ст. 12 Закону лише результат деталізації прав особи, гарантованих статтею 8 Закону. Ст. 25 Закону передбачає можливість обмеження дії ст. 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 ст. 8 Закону, слід застосовувати автоматично і до інших положень, що становить результат її деталізації, і в тому числі ст. 12. Інакше обмеження дії ст. 8 Закону втратило б будь-який сенс.

Тому, якщо інші закони встановлюють окремий порядок (більше обмежувальний, наприклад) повідомлення суб'єкта про збір інформації щодо нього і при цьому відповідають вимогам ст. 25 Закону, повинні застосовуватися саме положення таких законів. Яскравий приклад – положення Кримінального процесуального кодексу України, відповідно до яких підозрюваний ознайомлюється з усіма матеріалами провадження лише після завершення досудового розслідування.

В інших випадках (коли нема обмежень щодо обов'язку повідомляти) до того часу, як будуть внесені відповідні зміни до Закону, інформація, зазначена

---

101 Тут варто зазначити, що положення Директиви не застосовуються до обробки персональних даних у сфері оборони, національної безпеки та розслідування злочинів *(Прим. авт.)*

102 Якщо персональні дані отримуються від суб'єкта: суб'єктові вже відома інформація, що підлягає обов'язковому повідомленню, Якщо персональні дані отримано не від суб'єкта: суб'єктові вже відома інформація, що підлягає обов'язковому повідомленню; повідомлення потребуватиме докладення надмірних зусиль з боку володільця; збір чи розкриття персональних даних передбачено законом; якщо згідно із законодавством персональні дані повинні залишатися конфіденційними. *(Прим. авт.)*

в статті 12 Закону повинна надаватися суб'єктам в межах визначених у ній строків[103].

У зв'язку з цим постає ще одне питання, а саме щодо **форми повідомлення**. Закон визначає зобов'язання щодо сповіщення кожного суб'єкта про обробку, однак не встановлює форми такого повідомлення. Зрозуміло, що за певних умов таке зобов'язання буде надмірне. Тому допускається вжиття різних способів повідомлення, зокрема отримання підтвердження повідомлення від самого суб'єкта чи шляхом направлення однобічних повідомлень, чи розміщення інформації на вебсайті.

Важливо зазначити, що **саме на володільцеві 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 контрольному органові в ході перевірки. Її брак свідчитиме про невиконання володільцем своїх зобов'язань, закріплених у ст. 12 Закону.

Крім цього, відповідно до ч. 1 ст. 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 ч. 2 ст. 21 передбачено винятки з указаного правила у разі: «1) передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом; 2) виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом; 3) здійснення обробки персональних даних в історичних, статистичних чи наукових цілях; 4) повідомлення суб'єкта персональних даних відповідно до вимог частини другої статті 12 цього Закону»[104].

Вказане положення в Законі зайве і його слід видалити. Такі зобов'язання на володільців не покладаються жодним міжнародним документом. І це абсолютно правильно, бо, 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.

Положення частини другої статті 21 Закону можна використати при підготуванні 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

---

103 Слід зазначити, що як Директива, так і Регламент містять гнучкіші положення в частині, що стосується строків повідомлення. *(Прим. авт.)*

104 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр. 2010. 7 лип. (№ 122).*

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»[105], **слід зазначити, що вказане положення слід істотно доопрацювати**.

По-перше, жодного зобов'язання 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 для володільця. Фактично працівники володільця зобов'язані будуть повідомляти про кожну свою дію з персональними даними. По-третє, таке зобов'язання насправді не потрібне. О**сновна мета передбаченого ст. 12 Закону – зобов'язання володільця повідомляти про збір персональних даних суб'єкта – полягає в тому, щоб дати можливість суб'єктові орієнтуватися про, так би мовити, «ареал» поширення його персональних даних**. Знаючи, хто проводить їх обробку, та володіючи достатнім обсягом інформації про порядок такої обробки (див. ст. 12 Закону), суб'єкт може реалізувати решту своїх прав, гарантованих ст. 8 Закону. Наявність одного лише положення ст. 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.

Отже, володільцям рекомендується повідомляти суб'єктів персональних даних відомості, вказані в ст. 12 Закону, у момент збору їх персональних даних на умовах, визначених ч. 2 вказаного положення. Документи, які підтверджують факт такого повідомлення повинен в обов'язковому порядку зберігати володілець. Очевидні винятки з указаного правила становлять випадки, коли: 1) суб'єктові вже відомо про можливість такої передачі даних; 2) повідомлення кожного суб'єкта становитиме надмірний тягар. У такому разі володілець повинен вжити розумних заходів з метою доведення до відома всіх суб'єктів про факт отримання їхніх даних (наприклад, оголошення на вебсайті володільця); 3) можливість збору даних володільця передбачено законом або ж закон вимагає збереження факту передачі даних у таємниці. Володілець у таких випадках повинен бути готовий надати контрольному органові вичерпне пояснення щодо того, чому відповідне повідомлення не було направлене.

105 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

5.2. Право суб'єкта на доступ до своїх персональних даних

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

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»[106].

З указаного, а також принципу законності обробки, випливає, що **володілець повинен бути готовим у будь-який момент надати суб'єктові інформацію про те, на яких підставах (законних) проводиться обробка його персональних даних**, а отже і мати можливість пред'явити відповідний договір, документ, що засвідчує надання суб'єктом згоди, чи нормативно-правовий акт, що дає йому право обробляти персональні дані певного суб'єкта.

Важливе питання – доступ до інформації про джерела отримання персональних даних. Надання володільцем такої інформації пов'язане з запорукою дотримання принципу законності обробки. Лише надавши підтверджені доказами відомості про джерела отримання персональних даних, володілець зможе підтвердити законність їх обробки.

Загалом вказані положення достатньо чіткі та передбачувані. Певні суперечності викликає лише п. 2 ч. 2 ст. 8 Закону, відповідно до якого суб'єкт має право «отримувати інформацію про умови надання доступу до персональних даних, **зокрема інформацію про третіх осіб, яким передаються його персональні дані**». Часто вказане положення розуміється як таке, що стосується лише майбутніх можливих операцій із персональними даними. Насправді практика європейських держав[107] свідчить про те, що **суб'єкт має право на отримання**

---

106 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

107 Як і багато інших положень Закону воно взяте з Директиви, а саме статті 12 (a). *(Прим. авт.)*

відомостей про всі операції, які проводяться з його персональними даними (крім випадків, коли доступ до такої інформації обмежено законом).

У Директиві аналогічне право суб'єктів закріплене в статті 12 (a), відповідно до якої «Держави-члени гарантують кожному суб'єкту персональних даних право отримувати від володільця (a) без обмежень із розумними інтервалами та без надмірної затримки чи затрат (…) як мінімум інформацію щодо (…) отримувачів та категорій отримувачів, кому розкривають дані». У справі «*Мер і члени міської ради Роттердаму проти М. Е. Е. Ріджкебура*»[108] Суд Європейського Союзу надав тлумачення вказаного положення Директиви. Суд розв'язував питання про те, чи повинне вказане право (отримувати інформацію про одержувачів персональних даних суб'єкта) обмежуватися періодом один рік перед поданням суб'єктом запиту щодо отримання такої інформації. Суд вирішив, що «це право повинне обов'язково стосуватися минулого. Якби це було не так, суб'єкт персональних даних не зміг би ефективно реалізувати своє право на те, щоб його дані вважалися незаконно або неправильно виправленими, стертими чи заблокованими, або на подання позову до суду та отримання компенсації за завдані збитки». **Отже, володілець повинен автоматично зберігати інформацію про те, кому передавалися персональні дані суб'єкта, та за загальним правилом надавати її суб'єктові в разі його звернення**.

Чіткіше таке зобов'язання викладено в ст. 15 Регламенту. Згідно з п. 3 ч. 1 ст. 15 Регламенту суб'єкт персональних даних має право отримувати від володільця інформацію, серед іншого, про отримувачів чи категорії отримувачів, кому його персональні дані були чи будуть розкриті, зокрема отримувачів у третіх країнах та міжнародних організацій[109].

Детальніше порядок реалізації права на доступ до своїх персональних даних викладено в ст. 16 Закону (порядок доступу суб'єкта до інформації про себе). Частиною шостою вказаного положення визначено, що суб'єкт персональних даних має право на одержання будь-яких відомостей про себе в будь-якого суб'єкта відносин, пов'язаних із персональними даними, за умови надання інформації, визначеної в п. 1 ч. 4 ст. 16 Закону (прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит), окрім випадків, установлених законом.

Це положення в такому вигляді, як воно є тепер, видається недостатньо чітким та не забезпечує повною мірою прав суб'єкта на захист його персональних даних від незаконного доступу.

---

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

109 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.).

Призначення інформації, про яку йде мова в статті 16 Закону[110], – допомогти володільцеві знайти та надати правильні персональні дані (тобто дані особи запитувача). Однак ця інформація надає лише мінімальні гарантії верифікації особи запитувача у разі звернення в письмовому чи електронному вигляді (чи навіть особисто, але без пред'явлення документа, що посвідчує особу).

Не виникає запитань у разі особистого звернення суб'єкта, бо працівники володільця перевіряють документ, що посвідчує особу суб'єкта, та надають йому необхідну інформацію. Однак на практиці більшість суб'єктів звертається з письмовими запитами, у яких вказують зазначену в ч. 6 ст. 16 Закону інформацію, та вимагають надати доступ до їхніх персональних даних. Якщо інформація не має чутливого характеру, її надають. Разом із тим важко уявити ситуацію, коли суб'єкт звертається з письмовим запитом щодо отримання, наприклад, чутливої медичної інформації про себе і її йому надає адміністрація медичного закладу. Те саме стосується й інших видів чутливої інформації, наприклад тієї, що є в розпорядженні правоохоронних органів, телекомунікаційних компаній, банків тощо.

Частина 6 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**»[111]. Вказане обмеження передовсім слід розуміти так, що 1) закон може позбавляти особу доступу до її персональних даних (що загалом узгоджується з частиною першою ст. 25 Закону), а також, що 2) закон може встановлювати інші вимоги щодо обсягу інформації, яку повинен надавати суб'єкт для отримання доступу. Однак, по-перше, на цей момент далеко не всі галузеві закони містять положення щодо порядку доступу до персональних даних у відповідній сфері (наприклад, медицині, правоохоронній діяльності, телекомунікації тощо), а по-друге, це не розв'язує питання щодо форми запиту та відповіді.

Отже, положення щодо порядку доступу суб'єкта до його персональних даних повинні, з урахуванням характеру даних та особливостей певної сфери обробки, містити вимоги щодо форми запиту та відповіді (письмової, електронної, усної тощо), умов, за яких запитувана інформація надається, заходи щодо ідентифікації особи запитувача. Як альтернативу Закон повинен делегувати такі повноваження володільцям, які в такому разі повинні будуть самостійно з урахуванням персональних даних, що вони обробляють, розробляти процедуру доступу, яка повинна бути загальнодоступною.

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

---

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

111 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Як приклад можна навести практику застосування вказаного положення Уповноваженим ВРУ з прав людини.

Приклад. Практика розгляду скарг Уповноваженим ВРУ з прав людини

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

Частиною 1 статті 242 Цивільного кодексу України визначено, що батьки (усиновлювачі) – законні представники своїх малолітніх та неповнолітніх дітей[112]. 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 – їхня дитина[113].

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 в будь-якого суб'єкта відносин, пов'язаних із персональними даними, за умови надання інформації, визначеної в пункті 1 частини 4 цієї статті, крім випадків, установлених законом. Відповідно до пункту 1 частини 4 статті 16 цього Закону, в запиті щодо доступу до персональних даних зазначають: прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника)[114].

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[115].

112 Цивільний кодекс України № 435-IV від 16.01.2003 р. *Голос України*. 2003. 12 бер. (№ 45).

113 Про нотаріат : Закон України № 3425-XII від 02 вересня 1993 р. *Відомості Верховної Ради України*. 1993. 28 вер. (№ 39). Ст. 383.

114 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

115 Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України № 5492-VI від 20 листопада 2012 р. *Голос України*. 2012. 05 груд. (№ 231).

Крім цього, якщо мова йде про отримання відомостей про особу її законним представником, він повинен підтвердити наявність у нього таких повноважень. Відповідно до ст. 42 Цивільного процесуального Кодексу повноваження законних представників мають бути посвідчені, серед іншого, свідоцтвом про народження дитини[116].

Отже, для отримання запитуваної інформації про доньку, заявникові у своєму запиті до лікарні необхідно було вказати реквізити документа, що посвідчує його особу, а також підтвердити наявність у нього відповідних повноважень свідоцтвом про народження дитини. При цьому законодавством не визначено форми такого підтвердження. Вимога надати копії зазначених документів та копії свідоцтва про шлюб не передбачена чинним законодавством України.

Водночас слід взяти до уваги, що відповідно до статті 24 Закону володілець персональних даних (у цьому випадку – пологовий будинок) зобов'язаний забезпечити захист цих даних від випадкової втрати або знищення, незаконної обробки, зокрема незаконного знищення чи доступу до них.

Крім цього, відповідно до частини третьої статті 10 Закону, працівники володільця зобов'язані не допускати розголошення будь-яким способом персональних даних, які їм були довірені 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, яких повинен вживати володілець, визначає він самостійно та залежить переважно від чутливості персональних даних, які він обробляє.

Також слід наголосити, що в частині 6 статті 16 Закону мова йде саме про право доступу **суб'єкта персональних даних.**

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

Отже, з метою запобігання зловживанням, спрямованим на отримання конфіденційної інформації про особу (у цій справі мова йде про інформацію чутливого характеру) шляхом надсилання запиту від її імені, володілець персональних даних при наданні запитуваної інформації має

116 Цивільний процесуальний кодекс України № 1618-IV від 18 березня 2004 р. *Голос України*. 2004. 18 трав. (№ 89).

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 зробити шляхом зіставлення певних ідентифікаційних ознак особи, найпоширеніша з яких у справочинстві особистий підпис. Через те що для письмової форми звернення/запиту наявність особистого (власноручного) підпису обов'язкова, для перевірки особи запитувача при запитуванні інформації про себе допускається запитання разом із запитом копії сторінки документа, який посвідчує особу, що містить особистий підпис запитувача (наприклад, паспорт), що необхідно для проведення верифікації (встановлення справжності підпису шляхом візуального порівняння зі зразком).

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

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

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

Відповідно до ст. 8 Закону, суб'єкт має також право: «6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними; та… 11) відкликати згоду на обробку персональних даних»[117].

Щодо права особи пред'являти вимогу про знищення її персональних даних, це право деталізується в ст. 15 Закону, відповідно до якої «персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог

117 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

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 і володільцем чи розпорядником, якщо інше не передбачене законом[118]. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню в установленому законодавством порядку».

Крім цього, відповідно до частин першої та третьої ст. 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 (пп. 6 та 11 ч. 2 ст. 8 та ст. 15 Закону).

Щодо першого, важливе питання в цьому випадку – поняття **вмотивованості вимоги**, від чого практично залежить те, чи буде вона задоволена. У кожному разі володілець повинен розв'язувати це питання залежно від усіх обставин справи. Якщо мова йде, наприклад, про отримання суб'єктом рекламних повідомлень від володільця, то, щоб виправити неточності в імені чи інших даних, суб'єктові 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.

Щодо другого, слід зазначити у цьому зв'язку, що статті 8 (пп. 6 та 11 ч. 2 ст. 8) та 15 Закону неузгоджені між собою. Фактично поняття незаконності охоплює всі підстави видалення, передбачені ст. 15 Закону, та інші підстави для видалення персональних даних (наприклад, обробка без підстав, передбачених статтею 7 чи 11 Закону; обробка непропорційно великого обсягу даних тощо буде також незаконна). Отже, аналіз слід почати з підстав для видалення персональних даних, передбачених ст. 15 Закону.

1. Відповідно до ст. 15 Закону персональні дані видаляють після закінчення строку, на який особа дала згоду. Також, згідно з п. 11 ч. 2 ст. 8 Закону (див. вище), навіть якщо строки обробки, погоджені сторонами, не закінчилися, а особа відкликає згоду, такі дані все одно слід видалити. Отже, **особа має право вимагати видалення її персональних даних, коли строк обробки, на який вона давала згоду, закінчився або коли вона відкликає згоду на**

118 А також у разі: 3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) якщо набрало законної сили рішення суду щодо видалення або знищення персональних даних. Вказані підстави розглядатимуться в розділі, де йтиметься про порядок ведення контролю за додержанням законодавства про захист персональних даних. *(Прим. авт.)*

обробку персональних даних. Після закінчення вказаного строку чи відкликання згоди, якщо у володільця немає інших підстав для обробки даних, будь-яка подальша обробка буде незаконна[119].

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

Приклад

Особа уклала кредитний договір з банком. У такому разі банк зазвичай оброблятиме персональні дані особи на таких підставах, передбачених законом:

– згода: зазвичай банк бере в особи згоду на обробку її персональних даних для проведення цільового маркетингу, тобто рекламування своїх товарів і послуг. Строк такої згоди зазвичай невизначений;

– договір: на підставі положень договору банк оброблятиме персональні дані, необхідні для його виконання, 1) впродовж строку виконання договору та 2) певний час після його закінчення для захисту своїх інтересів від можливих скарг (зазвичай цей строк не перевищує строку позовної давності);

– закон: відповідно до Законів України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» та «Про банки і банківську діяльність», банк зобов'язаний ідентифікувати та верифікувати клієнта. З цією метою він має право на отримання низки необхідної з цією метою інформації та документів, які банк має право зберігати впродовж визначеного законом строку.

У 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 матиме права видалити персональні дані, необхідні для їх досягнення.

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

---

119 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Щодо такої передбаченої статтею 15 Закону підстави для видалення, як «припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачене законом», то вона доволі незрозуміла. Ймовірно, законодавець мав на увазі виконання сторонами зобов'язання/договору. Однак здебільшого припинення правовідносин не обов'язково тягне за собою видалення персональних даних. Наприклад, як ішлося 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. Тому, натепер 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 рішення суду щодо видалення або знищення персональних даних, що набрало законної сили, то детальніше вони розглянуті в розділі щодо ведення контролю за додержанням законодавства про захист персональних даних. Однак очевидно те, що вони також узгоджуються з положеннями ст. 8 Закону.

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

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

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

У разі, якщо суб'єкт доведе до відома державного органу, наприклад, те, що обробка його персональних даних не відповідає положенням Закону, то тому слід розглянути можливість вжиття заходів щодо перегляду відповідного нормативно-правового акта, на якому базується така обробка (такі заходи доцільні, коли порушення має системний характер. Коли мова йде про одиничний випадок, імовірно, слід передовсім видалити дані суб'єкта).

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

5.4. Право суб'єкта на заперечення проти обробки

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

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

12) знати механізм автоматичної обробки персональних даних;

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

П. 5 ч. 2 ст. 8 Закону видається схожим із пунктом 6 (вмотивована вимога щодо зміни чи знищення), однак призначення в нього зовсім інакше. Вказаний пункт був запозичений із Директиви, де він закріплює право особи у випадках, передбачених статтею 7 (e) та (f) Директиви (аналог пп. 2 та 6 ч. 1 ст. 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. Аналогічне положення міститься і в ст. 21 Регламенту.

Отже, якщо право на припинення обробки стосується даних, які обробляються незаконно, то в цьому разі мова йде про ситуації, коли елементу незаконності нема, однак **індивідуальні інтереси суб'єкта на захист його персональних даних переважають інтереси володільця щодо їх обробки**.

Ще один вагомий момент – право особи 1) на захист від автоматизованого рішення, яке має для неї правові наслідки та 2) знати механізм автоматичної обробки персональних даних.

Перше – по суті, право особи, виходячи з її індивідуальних обставин, заперечувати проти ухвалення такого автоматизованого рішення. Класичний приклад автоматизованого рішення – ситуація, коли, використовуючи надану особою інформацію, банк застосовує певний алгоритм, за допомогою якого автоматично оцінює її кредитоспроможність без урахування індивідуальних обставин (фактично особа розглядається як формальний набір сухих даних).

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

«Механізм автоматизованої обробки» традиційно називається профайлингом. Згідно з Регламентом, профайлинг – «будь-яка автоматизована обробка персональних даних, яка полягає у використанні персональних даних для того, щоб оцінити певні особисті аспекти фізичної особи, зокрема проаналізувати чи спрогнозувати працездатність особи, фінансову ситуацію, стан здоров'я,

споживацькі вподобання, інтереси, надійність, поведінку, місцезнаходження чи шляхи пересування».

Фактично це явище з погляду 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 має чутливіший характер. Наприклад, тривалий час купуючи товари в супермаркеті за допомогою отриманої картки покупця, суб'єкт передає володільцеві інформацію щодо зроблених закупів. Проаналізувавши таку інформацію (за допомогою певного алгоритму (механізму) автоматизованої обробки), володілець отримує додаткову інформацію щодо споживацьких вподобань, майнового стану та певних особистих звичок (наприклад, час та день закупів). Незалежно від подальшого використання такі дії становлять істотне 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). Наприклад, суб'єкт отримуватиме рекламу товарів, що відповідають його купівельній спроможності, чи товарів, що можуть його зацікавити. Також на підставі цієї інформації, яке може не завжди відповідати дійсності, ухвалюються рішення, які матимуть серйозні наслідки для прав та обов'язків суб'єкта. Якщо інформація, генерована внаслідок профайлингу, хибна, такі рішення можуть мати дискримінаційний характер.

Отже, 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. Тому, до проведення володільцем профайлингу+ повинні застосовуватися ті ж положення Закону, що й до решти даних, а саме: він повинен проводитися за згодою особи або на підставі закону, відповідати підставам законної обробки (див. ст. 7 та 11 Закону), відповідати принципам обробки персональних даних, інформації щодо проведення профайлингу повинна доводитися, як це передбачено ст. 8 Закону, до відома особи, щодо якої застосовуватиметься, тощо.

Крім цього, як уже зазначено вище, навіть якщо профайлинг законно застосовується, особа повинна мати можливість заперечити проти застосування в її ситуації його результатів.

Детальні рекомендації щодо проведення профайлингу викладено в Рекомендації КМ РЄ CM/Rec(2010)13. Згідно з указаним документом проведення профайлингу можливе за умови забезпечення суб'єктам персональних даних низки пов'язаних з цим гарантій. Як видно з указаної Рекомендації, ключові гарантії в цьому напрямку – 1) інформування суб'єктів щодо факту проведення

профайлингу, особи володільця, використовуваних персональних даних суб'єкта, механізму роботи профайлингу та результатів його застосування до персональних даних заявника 2) нагляд органів влади за проведенням володільцями профайлингу та 3) вжиття відповідних заходів з метою захисту персональних даних суб'єктів[120].

5.5. Інші права суб'єкта персональних даних

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

1) на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що невірогідні чи ганьблять честь, гідність та ділову репутацію фізичної особи;

2) звертатися зі скаргами щодо обробки своїх персональних даних;

3) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних[121]. Ці положення будуть детальніше розглянуті нижче.

Виходячи з цих норм, а також прав, розглянутих вище, суб'єкт має принаймні 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. У разі отримання відмови, яка, на думку суб'єкта, необґрунтована, він може звернутися до Уповноваженого чи суду. У такому разі його скарга до Уповноваженого буде обґрунтованіша та переконливіша (бо міститиме відповіді володільця). Окрім цього, в такому разі Уповноважений не потребуватиме додаткових документів, отримання яких займає більше часу, та за певних умов зможе відразу вжити необхідних заходів реагування.

Слід лише зазначити, що право застосовувати засоби правового захисту та звертатися зі скаргою передбачає не лише гарантії незалежного та безстороннього розгляду скарги та ухвалення рішення, здатного виправити порушення прав суб'єкта в разі, якщо воно сталося, а й імпліцитно гарантує особі можливості мати достатні ресурси для захисту своїх прав, тобто документи та

120 Див. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010). *(Прим. авт.)*

121 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

інформацію, що мають значення для розв'язання його справи. Це передбачає **обов'язок володільця детально фіксувати та документувати свою діяльність щодо обробки персональних даних** (див. також вище розділ про отримання суб'єктом даних щодо третіх осіб, яким передавалися персональні дані). Саме володілець повинен у разі направлення суб'єктом скарги мати можливість довести, що він не скоїв порушення, та надати відповідні докази. У зазначених вище гарантіях не було б 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 документів, що прямо заперечують його причетність до порушення прав суб'єкта чи демонструють, що він вжив усіх заходів, необхідних для запобігання скоєнню такого правопорушення, він повинен нести за це відповідальність.

5.6. Висновки

Зазначені вище права пов'язані та лише комплексне їх дотримання гарантує суб'єктові можливість контролювати обробку його персональних даних. Недотримання одних прав автоматично тягне за собою порушення інших.

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

2. Виходячи з отриманої інформації, він може самостійно звернутися до володільця та отримати детальнішу інформацію про обробку персональних даних

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

6. **ОБМЕЖЕННЯ ДІЇ ПРАВ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ**

Як уже йшлося вище в частинах, присвячених підставам обробки чутливих категорій персональних даних та прав суб'єкта на отримання інформації щодо обробки його персональних даних, реалізація всіх таких прав суб'єкта та принципів обробки персональних даних може обмежуватися на підставі статті 25 Закону. **Згідно з частиною 1 цієї статті** обмеження дії статей 6 (принципи обробки), 7 (обробка чутливих категорій персональних даних) і 8 (права суб'єкта персональних даних) Закону може відбуватися у випадках, передбачених законом, скільки це необхідно в демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб[122]. Слід зазначити, що такий перелік обмежень відповідає змістові статті 8 Європейської конвенції з прав людини, яка встановлює, що втручання у право на приватність можливе, коли воно відбувається «згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб»[123].

Отже, обмеження дії вказаних положень Закону можливе, лише якщо:

1) передбачене законом;

2) необхідне в демократичному суспільстві і відбувається пропорційно до встановленої мети;

3) переслідує одну з легітимних цілей: захист національної безпеки, економічного добробуту або захисту прав і свобод суб'єктів персональних даних чи інших осіб.

У зв'язку з цим виникає дещо цікава та парадоксальна ситуація: виходить, що обмеження застосування принципів законності, легітимної мети та необхідності повинні своєю чергою, бути законними, необхідними та переслідувати легітимну мету. Очевидно, що такий, на перший погляд, рекурсивний підхід має на меті гарантувати максимальну збалансованість та об'єктивність при обмеженні прав людини і типовий для всього каталогу прав людини першого покоління.

---

122 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

123 Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 р. *Голос України*. 2001. 10 січ. (№ 3).

Відповідно, вищевказане свідчить про те, що фактично **не може бути ніяких обмежень до принципів легітимної мети, необхідності та законності**. Вказані принципи – зобов'язання володільця, яких він повинен дотримуватися за будь-яких умов.

Разом із тим не виникає жодного сумніву, що за умови дотримання положень статті 25 Закону можна обмежити застосовність принципу прозорості, відкритості, прав суб'єкта персональних даних, а також відступити від положень статті 7 Закону. 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 Закону «Основи законодавства України про охорону здоров'я», за загальним правилом, пацієнт, який досяг повноліття, має право на отримання вірогідної і повної інформації про стан свого здоров'я, зокрема на ознайомлення з відповідними медичними документами, що стосуються його здоров'я (частина перша статті 39)[124].

Разом із тим, відповідно до частини четвертої статті 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[125].

Цим положенням закону (частиною 4) обмежується право особи на ознайомлення з інформацією про себе. Однак таке обмеження, встановлене законом (частина 4 статті 39), переслідує легітимну мету (захист прав пацієнта або інших осіб) та необхідне для її досягнення (інакше (мається на увазі в разі надання інформації) може бути завдана шкода здоров'ю пацієнта/інших осіб, виникнуть перешкоди належному лікуванню).

Щодо **обмеження державним органом доступу суб'єкта до його персональних даних**, то тут слід зважувати одночасно положення кількох законів. Передусім, згідно зі статтею 32 Конституції України, «Кожний громадянин має право знайомитися в органах державної влади, органах місцевого

124 Основи законодавства України про охорону здоров'я : Закон України від 19 листопада 1992 р. № 2801-XII. *Відомості Верховної Ради України.* 1993. 26 січ. (№ 4).

125 Основи законодавства України про охорону здоров'я : Закон України від 19 листопада 1992 р. № 2801-XII. *Відомості Верховної Ради України.* 1993. 26 січ. (№ 4).

самоврядування, установах і організаціях з відомостями про себе, які не є **державною або іншою захищеною законом таємницею**»[126].

Згідно зі статтею 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». Відповідно до частини другої статті 6 цього Закону, обмеження доступу до інформації робиться відповідно до закону при дотриманні сукупності таких вимог:

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

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес у її отриманні[127].

Звідси випливає, що доступ особи до інформації про себе обмежується лише на **підставі закону** (стаття 6 та 8 Закону України «Про доступ до публічної інформації»), для **цілей та на умовах, передбачених пунктом 1 частини другої статті 6 вказаного Закону**. Вказані цілі повністю відповідають тим, що передбачені статтею 25 Закону (хоч перелік цілей дещо відрізняється). Пункти 2 та 3 частини другої статті 6 Закону України «Про доступ до публічної інформації» – деталізованіший варіант принципу необхідності, про який мова йде у статті 25 Закону.

126 Конституція України від 28 червня 1996 р. № 254к/96-ВР. *Голос України*. 1996. 13 лип. (№ 128).

127 Про доступ до публічної інформації : Закон України від 13 січня 2011 р. № 2939-VI. *Голос України*. 2011. 09 лют. (№ 24).

7. ПОРЯДОК ОРГАНІЗАЦІЇ ВОЛОДІЛЬЦЕМ ПРОЦЕСУ ОБРОБКИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

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

Поняття захисту персональних даних доволі широке та зазвичай охоплює два ключові елементи:

- **зобов'язання володільця** вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних (стаття 24 Закону);
- **зобов'язання кожного працівника** володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних, чи службових, чи трудових обов'язків, так зване зобов'язання конфіденційності (стаття 10 Закону)[128].

Володілець персональних даних самостійно повинен визначати, яких заходів слід вживати з метою забезпечення захисту персональних даних. У будь-якому разі, такі заходи повинні бути пропорційними до потенційних ризиків, пов'язаних з обробкою персональних даних, що проводить володілець.

Перелік обов'язкових заходів захисту, яких повинні вживати всі володільці, визначено Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого від 08.01.2014 № 1/02-14. Ці вимоги мають загальний характер і це мінімальні вимоги у сфері захисту персональних даних, а шляхи їх практичної імплементації вирішує в індивідуальному порядку кожен окремий володілець.

128 Про захист персональних даних : Закон України від 23.04.2021 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Організаційні заходи із захисту персональних даних згідно з Типовим порядком від 08 січня 2014 року

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;

– розроблення 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, чи 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 були довірені або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

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

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

3.10. У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику.

(…)

3.14. З метою убезпечення обробки персональних даних вживаються спеціальні технічні заходи захисту, зокрема щодо унеможливлення несанкціонованого доступу до персональних даних, що обробляються, та роботи технічного і програмного комплексу, за допомогою якого проводиться їх обробка.

(…)[129]

Отже, передовсім 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 володільцеві (залежно від масштабу діяльності, кількості його працівників) доцільно визначити типові рівні доступу.

Приклад

Підприємство веде базу даних, у яку вносяться такі дані клієнтів:

1) прізвище, ім'я та по батькові, 2) рік, дата народження та вік, 3) телефон/електронна адреса, 5) адреса проживання, 6) місце роботи (сфера зайнятості), 7) дані про склад сім'ї, 8) дані про придбані товари.

Доступ до бази даних передбачається надавати на 4-х рівнях:

керівник – доступ до всіх категорій даних;

спеціаліст-маркетолог (розроблення 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 доставлення товару) – доступ до 1, 2, 3 категорії даних;

спеціаліст з роботи з постійними клієнтами – доступ до 1–8 категорії даних.

Отже, якщо ретельно розмежовувати рівні доступу, з персональними даними працюватиме лише невелика кількість працівників.

129 Про затвердження документів у сфері захисту персональних даних : Наказ № 1/02-14 від 08.01.2014 р. *Баланс*. 2014, 06 бер. 2014. № 19. Ст. 5.

Перед отриманням доступу до персональних даних кожен працівник повинен пройти процедуру ідентифікації/автентифікації, зокрема шляхом особистого введення індивідуального та відомого лише йому пароля (чи іншим способом, наприклад шляхом використання індивідуальної картки, яка автоматичну запускає визначені для конкретного користувача налаштування тощо). 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 у системі, за допомогою присвоєного їм ідентифікатора.

Володілець може вести контроль доступу до приміщень, де зберігаються картотеки/сервери з персональними даними, та робочих приміщень загалом. Залежно від важливості інформації, що зберігається в базі даних, приміщення можуть обладнуватися автоматичними електронними замками, сигналізацією тощо. Як додатковий захід безпеки, володільці можуть (з дотриманням певних гарантій) із метою контролю за виробничою дисципліною, дотриманням правил трудової етики наглядати за працівниками.

Якщо володілець проводить автоматизовану обробку 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 так, щоб позбавити працівників можливості вводити зайві обсяги персональних даних і проводити недопустимі операції з обробки (наприклад, несанкціоноване копіювання, друк тощо) або ж контролювати такі процеси. Саме програмне забезпечення має, по змозі, встановлювати строки збереження інформації та в разі їх закінчення автоматично її видаляти.

Вказані вимоги відповідають правилу захисту персональних даних *за умовчанням* (англ. *privacy by default*), визнаному правилу у сфері захисту персональних даних у Європейському Союзі. Стаття 25 Регламенту передбачає, що володілець зобов'язаний впроваджувати механізми гарантування того, що за замовчуванням обробляються лише ті персональні дані, які необхідні 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[130].

130 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.).

Проте простого впровадження цих механізмів недосить: їх повинні супроводжувати додаткові заходи, покликані забезпечити їх реальну ефективність. Наприклад, володілець повинен забезпечити і регулярне навчання своїх працівників, їх ознайомлення з порядком обробки персональних даних та отримати від них зобов'язання щодо збереження конфіденційності інформації тощо.

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 детальніші вимоги щодо технічного захисту інформації. Слід зазначити, що ці вимоги доволі жорсткі та не враховують особливостей того чи іншого володільця (зокрема, його фінансових можливостей, масштабів обробки персональних даних, характеру даних тощо).

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

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 авдиту, 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, зокрема, права направити скаргу до Уповноваженого чи суду), а також компетенції Уповноваженого (частина друга статті 8 та стаття 23 Закону). Право особи на захист своїх прав не матиме сенсу в разі, якщо неможливо буде встановити хто, коли, яким способом обробляв та кому передавав його персональні дані.

Правильність саме такого тлумачення норм чинного законодавства підтверджується практикою Суду Європейського Союзу, щодо тлумачення відповідних норм Директиви (див. вище в розділі про права суб'єкта персональних даних рішення Суду справедливості ЄС у справі «*Мер і члени міської ради*

Роттердаму проти М. Е. Е. Ріджкебура»[131]). Також вказане зобов'язання передбачено Регламентом у частині 2 статті 5 та статті 30[132].

У зв'язку з цим та на виконання вказаних вище положень Закону Уповноважений у пункті 3.11 Типового порядку обробки персональних даних передбачив обов'язок володільця вести **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 і доступом до них. З цією метою володілець/розпорядник зберігає інформацію 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 зробив одну з 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 разі обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Її володілець/розпорядник зберігає протягом одного року з моменту закінчення року, у якому виконано зазначені операції, якщо інше не передбачено законодавством України.

(…)

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

132 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.).

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

Приклад 1. Справа «I. v. Finland»[133]

До Європейського суду з прав людини звернулася особа, що була хвора на СНІД. Вона проходила лікування в лікарні, де вона і працювала. У певний момент інформація про діагноз заявниці стала відомою широкому колу працівників лікарні. Вона звернулася по захист своїх прав до суду. Їй відмовили в задоволенні скарг. Суди визнали, що інформацію незаконно поширив хтось із працівників лікарні. Однак інформацію щодо того, хто міг це зробити, зокрема, хто переглядав дані заявниці, лікарня не зберігала. 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 причиново-наслідкового зв'язку між недоліками в правилах доступу та поширенням інформації про стан її здоров'я. Цілком очевидно, що якби лікарня забезпечила сильніший контроль над доступом до медичних карток, зробивши їх доступними лише для медперсоналу, який безпосередньо був залучений до лікування заявниці, або запровадила ведення обліку всіх осіб, які мали доступ до медичної картки заявниці, остання мала б вигідніші позиції під час проваджень у національних судах. На думку Суду, вирішальний 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 опрацьовуваних записах, відповідним чином захищена від незаконної обробки, використання, знищення, зміни або викрадення), і саме цьому фактові національні суди не приділили належної уваги». Суд дійшов висновку, що була порушена стаття 8.

Приклад 2. Практика Уповноваженого ВРУ з прав людини

2015 року до Уповноваженого звернулася заявниця зі скаргою про те, що працівники лікарні її повідомили про те, що її медична картка зникла з поліклініки.

У зв'язку із зазначеною скаргою Уповноважений відкрив провадження, у межах якого направив вимогу про надання коментарів щодо скарги заявниці керівникові поліклініки. Крім цього, Уповноважений запитав інформацію щодо того, чи зберігається/лася в поліклініці медична картка

133 «*I. v. Finland*», заява № 20511/03.

заявниці, і якщо так, то кому та коли її востаннє передавали. Вказану інформацію слід було підтвердити відповідними документами.

Лікарня повідомила, що медична картка є в самої заявниці.

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

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

У зв'язку з цим Уповноважений констатував 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'єктові чи Уповноваженому вичерпну інформацію щодо того, чи обробляв він персональні дані суб'єкта, а також, коли та кому їх передавали.

– 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 достатньою мірою захистити персональні дані суб'єктів від незаконних дій, якщо він не володіє інформацією щодо того, якими даними він володіє та хто має до них доступ.

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

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

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

Актуалізація питань захисту та обробки персональних даних способом, який відповідає визнаним стандартам у цій сфері викликає потребу в посиленні інституційних механізмів контролю в цій сфері. В окремому розділі цього посібника ми розглянемо питання, пов'язані з офіційним публічним (державним) контролем у цій сфері, тому тут зупинимося на тих механізмах, які існують та діють в окремих установах та організаціях, незалежно від форми власності, а саме особах та структурних підрозділах, відповідальних за захист персональних даних.

Відповідно до частини другої статті 24 Закону, **в органах державної влади, органах місцевого самоврядування**, (…) створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану зі захистом персональних даних при їх обробці. Основне завдання такої посадової особи полягає в тому, щоб налагодити належним чином роботу з персональними даними, що обробляє володілець/розпорядник, чи вжити всіх можливих заходів з метою налагодження такої роботи (бо останнє слово все ж залишається за керівництвом володільця-розпорядника).

Компетенцію та повноваження такої особи чи підрозділу зазвичай самостійно визначає володілець у своїх внутрішніх документах. Законодавство надає лише їх мінімальний перелік. Нижче подано розширений перелік типових функцій та повноважень структурного підрозділу/відповідальної особи, які повинні забезпечити належне виконання покладених на них завдань. Зазвичай такі функції передбачають необхідність:

1) Оцінювати ризики від обробки персональних даних володільцем і надавати з урахуванням проведеного оцінення консультації володільцеві щодо

належної організації процесу обробки персональних даних (і документувати цю діяльність).

З цією метою відповідальна особа/підрозділ насамперед повинна, виходячи з того, яка мета обробки персональних даних володільцем, склад персональних даних, категорії суб'єктів персональних даних та операції з обробки, які проводить (планує) володілець, оцінити потенційні ризики від таких операцій. Зокрема, чи істотною буде шкода, завдана суб'єктові, від втрати (видалення) таких даних, їх незаконного чи випадкового поширення, а також чи сильна мотивація у працівників володільця, третіх осіб намагатися отримати ці дані чи незаконно комусь передати.

Виходячи з проведеного оцінення, відповідальна особа чи структурний підрозділ розробляє пропозиції щодо порядку захисту персональних даних, роботи із запитами суб'єктів і третіх осіб, визначення оптимального складу даних, що підлягатиме обробці, порядку збору персональних даних і повідомлення про це суб'єкта, порядку та рівнів доступу працівників до персональних даних, порядку документування процесів, пов'язаних з обробкою персональних даних тощо. З цією метою в державних органах така відповідальна особа повинна бути залучена до всіх процесів, пов'язаних з розробкою нормативно правових актів, що регламентуватимуть порядок обробки персональних даних володільцем.

2) Консультувати в разі необхідності інші підрозділи володільця щодо розгляду запитів суб'єктів і третіх осіб про отримання доступу до персональних даних.

3) Проводити моніторинг процесів обробки персональних даних на предмет їх відповідності до законодавства та Закону. Відповідальна особа чи структурний підрозділ може проводити авдит дотримання володільцем чи розпорядником законодавства про захист персональних даних. У разі виявлення порушень, а саме недотримання законодавства чи недоліків у самому законодавстві, доводити результати роботи до відома керівництва з рекомендаціями щодо усунення вказаних проблем.

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

5) Ознайомлювати керівництво та працівників володільця з вимогами чинного законодавства про захист персональних даних, змінами до законодавства, актуальними питаннями обробки персональних даних у сфері діяльності володільця, організовувати відповідні навчання для працівників.

б) Взаємодіяти з Уповноваженим, що може проявлятися в таких основних напрямках: а) консультації з приводу доцільності та порядку обробки персональних даних володільцем, отримання з цього приводу роз'яснень Уповноваженого; б) направляти Уповноваженому для погодження розроблені проєкти нормативно-правових актів, що стосуються питань обробки персональних даних); в) співпрацювати в ході проведення Уповноваженим перевірки володільця (забезпечення швидкого надання всієї інформації щодо обробки персональних даних володільцем, супровід у ході проведення перевірки, забезпечення вільного доступу до всіх приміщень, де проводиться обробка персональних даних, та безпосередньо до інформації (і зокрема персональних даних), що її обробляє володілець, тощо); г) забезпечення вчасного та повного виконання приписів Уповноваженого.

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

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

2) щодо доступу до всієї інформації та документів, що стосуються обробки персональних даних, яку проводить володілець чи розпорядник, зокрема персональних даних, що містяться в базах даних володільця, журналу реєстрації обліку операцій, пов'язаних з обробкою персональних даних тощо;

3) завчасно отримувати повну інформацію щодо будь-яких операцій, пов'язаних з обробкою персональних даних, що планує володілець/розпорядник;

4) правом безпосереднього звітування керівництву володільця чи розпорядника.

Важливий момент у цьому контексті також те, що покладення таких функцій на відповідну особу чи структурний підрозділ не може бути автоматичним чи номінальним. Для виконання вказаних вище завдань і функцій відповідальна особа чи працівники відповідного підрозділу повинні володіти відповідними навичками та досвідом, зокрема відповідною кваліфікацією у сфері захисту персональних даних і безпеки інформації.

Для цього рекомендується наявність у неї відповідної освіти чи проходження такою особою відповідного спеціалізованого навчання. Законодавство не встановлює об'єктивних вимог і критеріїв щодо конкретних видів освіти чи кваліфікацій, які мають бути в таких осіб, проте очевидно, що це залежатиме від специфіки діяльності конкретних установ та організацій, типів та обсягів персональних даних, які вони обробляють тощо.

Вимога щодо підготування таких уповноважених осіб насправді достатньо значуща. У разі витоку персональних даних чи іншого порушення порядку їх обробки, саме брак відповідного підготування персоналу чи кваліфікацій

у відповідальних осіб і представників структурних підрозділів володільця та розпорядника буде одним із факторів для встановлення ступеня вини.

Законодавство, внутрішньовідомчі документи та посадова інструкція таких відповідальних осіб або ж положення про структурний підрозділ повинні гарантувати їхню незалежність і безсторонність. Для цього рекомендується, щоб обов'язки щодо організації процедури захисту персональних даних були покладені 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 із захистом персональних даних. Крім цього, така особа має бути забезпечена всіма необхідними (зокрема фінансовими та людськими) ресурсами для ефективного виконання нею своїх обов'язків. Керівники володільця не мають права примушувати відповідальних осіб до надання тих чи інших рекомендацій чи виконання певним чином їхніх обов'язків у сфері захисту персональних даних.

7.3. Порядок організації володільцем процесу обробки персональних даних

За загальним правилом, обробку персональних даних володілець здебільшого проводить, якщо вона необхідна для виконання завдань такого органу, покладених на нього обов'язків та належної організації власної роботи. Будь-яка обробка персональних даних державним органом повинна бути законною.

Згідно з принципом законності:

- проведення обробки персональних даних повинно базуватися на положеннях закону;
- порядок обробки повинен регламентуватися законодавством.

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

1) інформацію про володільця персональних даних. Якщо їх декілька – інформацію про кожного, а також співвідношення їхніх повноважень;
2) інформацію про розпорядника персональних даних (у разі наявності);
3) мету обробки персональних даних (див. детальніше вимоги щодо формулювання мети в параграфі 3.2);
4) категорії суб'єктів, чиї персональні дані обробляють;
5) склад персональних даних, що їх обробляють;

6) порядок і спосіб збору персональних даних;

7) порядок верифікації та видалення персональних даних;

8) строк зберігання персональних даних;

9) гарантії дотримання прав суб'єктів персональних даних:

   – порядок реалізації права суб'єкта на доступ до своїх персональних даних;

   – порядок надання інформації щодо порядку обробки персональних даних;

   – порядок надання інформації щодо того, яким третім особам передавали дані;

   – порядок розгляду звернень щодо видалення чи зміни персональних даних;

   – порядок розгляду заперечень проти обробки персональних даних;

   – порядок розгляду скарг на незаконність обробки персональних даних;

10) третіх осіб, яким передають / яким надають доступ до персональних даних;

11) проведення транскордонної передачі даних (у разі наявності): підстави, порядок та отримувачів;

12) технічні та організаційні засоби захисту персональних даних (нижче наведено приблизний перелік):

   – розмежування рівнів доступу працівників володільця до персональних даних та їхніх повноважень щодо обробки;

   – порядок та умови отримання працівниками доступу до персональних даних;

   – ведення обліку операцій обробки персональних даних (фіксація в журналі відомостей щодо особи, яка проводить операцію, характер дій щодо персональних даних (перегляд, копіювання, друк, передача тощо), щодо яких персональних даних, час таких дій тощо);

   – псевдонімізація та криптографічний захист персональних даних;

   – тестування та оновлення системи технічного захисту;

   – інше.

13) алгоритм дій на випадок випадкової втрати чи зміни персональних даних, їх незаконної обробки[134].

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

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

---

134 Про захист персональних даних : Закон України від 23.04.2021 р. №2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122); Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних : Затверджено Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення: 23.05.2021).

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

8.1. Еволюція інституційного механізму контролю за додержанням законодавства про захист персональних даних в Україні

Інституційний механізм публічного контролю у сфері захисту персональних даних – важливий механізм реалізації відповідних законодавчих стандартів і дієвості гарантій, які встановлено для суб'єктів персональних даних. Створення та діяльність такого механізму – важлива частина міжнародних стандартів захисту персональних даних. У статті 1 Додаткового протоколу до Конвенції 108 передбачено зобов'язання сторін Конвенції створити «один чи більше органів нагляду, відповідальних за забезпечення дотримання заходів, які передбачено її внутрішньодержавним правом і які втілюють принципи, викладені в… Конвенції та в цьому Протоколі»[135].

До повноважень таких органів згідно з Протоколом мають належати:

- розслідування та втручання у разі порушення законодавства про захист персональних даних;
- право брати участь у судовому розгляді порушення законодавства про захист персональних даних;
- повідомляння компетентних судових органів про порушення законодавства про захист персональних даних;
- ухвалення рішення у зв'язку із заявами будь-якої особи про захист її прав та основоположних свобод стосовно обробки персональних даних;
- співпраця з уповноваженими органами інших держав такою мірою, якою це необхідно для виконання їхніх обов'язків, зокрема шляхом обміну будь-якою корисною інформацією[136].

135 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 року. *Офіційний вісник України*. 2011. 14 січ. (№ 1(58)).

136 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 року. *Офіційний вісник України*. 2011. 14 січ. (№ 1(58)).

Крім вимог Додаткового протоколу, на відповідні механізми поширюється також дія деяких інших міжнародних гарантій і стандартів у сфері захисту прав людини, зокрема – Паризькі принципи, які стосуються статусу національних установ, що займаються заохоченням і захистом прав людини, ухвалені 9 жовтня 1991 року та затверджені Резолюцією Генеральної Асамблеї ООН № 48/134 від 20 грудня 1993 року (надалі – Паризькі принципи).

Європейський Союз теж визнає незалежність контрольного органу як важливий критерій його функціонування. Регламент у ст. 52(1) встановлює, що: «Кожний наглядовий орган діє абсолютно незалежно під час виконання своїх завдань і здійснення своїх повноважень згідно з цим Регламентом»[137]. Європейські експерти теж зазначають, що «Незалежність контрольного органу та його членів і працівників від прямих або непрямих зовнішніх впливів – основна гарантія повної об'єктивності при розв'язанні питань щодо захисту даних»[138].

Створення відповідного інституційного механізму було передбачене Законом "Про захист персональних даних" 2010 р. Проте формальне створення цього механізму розтягнулося майже на рік після ухвалення Закону. Першим органом, який був наділений контрольними повноваженнями у сфері захисту персональних даних згідно з профільним Законом, стала Державна служба України з питань захисту персональних даних (надалі – ДСЗПД), створена на підставі Указу Президента «Про Положення про Державну службу України з питань захисту персональних даних» від 06 квітня 2011 року № 390/2011. Відповідно до нього, ДСЗПД була центральним органом виконавчої влади, який забезпечував реалізацію державної політики у сфері захисту персональних даних[139].

Серед основних завдань ДСЗПД згідно із положенням були визначені:

1) внесення пропозицій щодо формування державної політики у сфері захисту персональних даних;
2) реалізація державної політики у сфері захисту персональних даних;
3) контроль за додержанням вимог законодавства про захист персональних даних;
4) здійснення міжнародно-правового співробітництва у сфері захисту персональних даних[140].

---

137 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021).

138 Посібник з європейського права у сфері захисту персональних даних 2018. К.: К.І.С., 2020. С. 201.

139 Про Положення про Державну службу України з питань захисту персональних даних: Указ Президента України від 06 квітня 2011 року № 390/2011, *Урядовий кур'єр*. 2011. 21 квіт. (№ 73).

140 Про Положення про Державну службу України з питань захисту персональних даних: Указ Президента України від 06 квітня 2011 року № 390/2011, *Урядовий кур'єр*. 2011. 21 квіт. (№ 73).

Від початку діяльності ДСЗПД вона піддавалася критиці з боку правозахисників та міжнародних організацій і проєктів. Причиною цього була глибока інтегрованість Служби в систему органів виконавчої влади. Міжнародно визнаний ключовий принцип функціонування контрольних органів у цій сфері – їхня незалежність, зокрема відносно органів виконавчої влади. Це пов'язано з тим, що дуже часто саме органи цієї гілки влади стають головними порушниками норм і стандартів щодо захисту та обробки персональних даних.

Відповідний стандарт закріплено й у статті 1 Додаткового протоколу до Конвенції 108, у якій закріплено, що органи нагляду у сфері захисту персональних даних «виконують свої функції цілком незалежної»[141]. На гарантіях незалежності також наголошується у вищезгаданих Паризьких принципах, як загальна вимога до органів із захисту прав людини незалежно від фокусу їхньої діяльності[142].

Водночас ДСЗПД, що, як уже йшлося вище, за своєю природою належала до центральних органів виконавчої влади, не відповідала стандартові незалежності. Відповідно до пункту 1 Положення, Служба де факто перебувала в системі Мін'юсту і передбачалося, що її діяльність: «спрямовується і координується Кабінетом Міністрів України через Міністра юстиції України»[143]. Також варто відзначити, що Голову ДСЗПД, згідно із п. 9 Положення, призначав на посаду за поданням Прем'єр-міністра України, внесеним на підставі пропозицій Міністра юстиції України, та звільняв з посади Президент України[144]. Такий статус-кво передбачав парадоксальні ситуації, коли Служба теоретично могла б проводити перевірки навіть самого Мін'юсту і виносити приписи його керівництву, тому поставали обґрунтовані сумніви в ефективності та об'єктивності цього механізму. Така внутрішньоорганізаційна незалежність теж важливий стандарт діяльності контрольних механізмів на думку і європейських експертів: «Не лише закон, який передбачає створення органу, має містити конкретні гарантії незалежності, але й організаційна структура цього органу повинна демонструвати незалежність»[145].

---

141 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 року. *Офіційний вісник України*. 2011. 14 січ. (№ 1(58)).

142 Principles relating to the Status of National Institutions (The Paris Principles) : Adopted by General Assembly resolution 48/134 of 20 December 1993. URL: https://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx (Date of request: 16.05.2021).

143 Про Положення про Державну службу України з питань захисту персональних даних: Указ Президента України від 06 квітня 2011 року № 390/2011, *Урядовий кур'єр*. 2011. 21 квіт. (№ 73).

144 Про Положення про Державну службу України з питань захисту персональних даних : Указ Президента України від 06 квітня 2011 року № 390/2011, *Урядовий кур'єр*. 2011. 21 квіт. (№ 73).

145 Посібник з європейського права у сфері захисту персональних даних 2018. К.: К.І.С., 2020. С. 201.

Правовий статус та діяльність ДСЗПД зазнавали критики і з боку широкого кола експертів і дослідників. Як наголошувала визнана міжнародна експертка у сфері захисту персональних даних Марі Жорж, «цей орган не діє незалежно, що є абсолютно необхідно, особливо тому, що обробка даних вестиметься як у приватному, так і в державному секторі, зокрема стосовно спецслужб»[146]. Своєю чергою, І. М. Сопілко висловлював обґрунтовані застереження стосовно того, що Службі надано «занадто широкі повноваження». А також він вказував на «відсутність належного нормативно-правового регулювання порядку проведення та механізмів проведення перевірок»[147].

Інший міжнародний експерт, Грем Саттон, підкреслював, що: «Відсутність незалежності органу нагляду – один із найсерйозніших недоліків цього Закону». Також він зазначав, що: «Незалежність суттєво необхідна для забезпечення безперечного виконання органами нагляду свого обов'язку контролювати та забезпечувати додержання законодавства про захист даних усіма організаціями, зобов'язаними Законом, зокрема з урядом»[148].

Проблеми з незалежністю не були єдиною причиною критики ДСЗПД. Марі Жорж критикували її статус у зв'язку із:

- можливістю втручання Служби до обробки даних, які заявлені до реєстрації;
- неясністю щодо можливостей оскарження адміністративних рішень Служби в судовому порядку;
- непрозорістю діяльності Служби та браком вимоги публікації щорічного звіту[149].

У зв'язку із цим 3 липня 2013 року Верховна Рада України ухвалила Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», згідно із яким повноваження щодо ведення контролю за додержанням законодавства про захист персональних даних були передані Уповноваженому ВРУ з прав людини (надалі – Уповноважений)[150]. Українські дослідники О. В. Гронь та А. К. Погореленко, коментуючи ухвалення закону, підтверджують вищенаведену тезу, що це стало наслідком «прагнення законотворців запровадити європейські підходи

146 Жорж М., Саттон Г. Аналіз Закон України «Про захист персональних даних». Страсбург, 2012. С. 19.

147 Сопілко І. М. Механізм захисту персональних даних: проблеми та перспективи. *Юридичний вісник. Повітряне і космічне право*. 2013. № 2.

148 Жорж М., Саттон Г. Аналіз Закон України «Про захист персональних даних». Страсбург, 2012. С. 41.

149 Жорж М., Саттон Г. Аналіз Закон України «Про захист персональних даних». Страсбург, 2012. С. 19.

150 Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України №383-VII від 03 липня 2013 р. *Урядовий кур'єр*. 2013. 31 лип. (№ 136).

до захисту прав людини»[151]. І. М. Сопілко аналогічно оцінював передання повноважень контролю в цій сфері до Уповноваженого як «позитивне явище»[152].

Основними відмінностями статусу Уповноваженого, як контрольного органу у сфері захисту персональних даних від статусу ДСЗПД, які давали достатні гарантії незалежності його діяльності відповідно до Додаткового протоколу до Конвенції 108 і Паризьких принципів, стали:

- спосіб призначення (Уповноваженого призначає на посаду і звільняє з посади Верховна Рада України таємним голосуванням шляхом подання бюлетенів);
- термін перебування на посаді та умови припинення виконання обов'язків (Уповноваженого призначає строком на п'ять років. Верховна Рада України ухвалює рішення про звільнення з посади Уповноваженого до закінчення строку або в інших випадках передбачених законом;
- спосіб ухвалення рішення (заборонено втручання органів державної влади, органів місцевого самоврядування, об'єднань громадян, підприємств, установ, організацій незалежно від форми власності та їхніх посадових і службових осіб у діяльність Уповноваженого).

Також слід зазначити, що були розв'язані й інші проблеми, на яких наголошувала і Марі Жорж. Зокрема, була передбачена можливість оскарження рішень (приписів) Уповноваженого в судовому порядку, а звітування про виконання функцій Уповноваженого у сфері захисту персональних даних стало вноситися до щорічних звітів Уповноваженого про стан дотримання прав і свобод людини і громадянина в Україні.

Зміни, ухвалені Верховною Радою 3 липня 2013 року, набрали чинності 1 січня 2014 року. Проте Секретаріат Уповноваженого в щорічній доповіді за 2013 рік ставив собі за ціль: «сформувати ефективну систему моніторингу виявлення та усунення порушень у сфері обробки персональних даних та подальшого контролю за дотриманням законодавства з питань захисту персональних даних»[153]. Як елементи такої майбутньої системи визначено:

- розгляд звернень громадян, що надходять до Уповноваженого;
- аналіз судових рішень, які стосуються захисту персональних даних;
- впровадження заходів контролю шляхом проведення перевірок суб'єктів відносин при обробці персональних даних[154].

---

151 Гронь О., Погореленко А. Проблеми захисту персональних даних у контексті сучасної комунікації. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2018. Вип. 19(1). С. 104.

152 Сопілко І. М. Механізм захисту персональних даних: проблеми та перспективи. *Юридичний вісник. Повітряне і космічне право*. 2013. № 2. С. 69.

153 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. – К., 2013. – С. 265-266.

154 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. – К., 2013. – С. 266.

З цією метою та для цілей реалізації вказаних повноважень із контролю за додержанням законодавства у сфері захисту персональних даних Уповноважений запровадив посаду Представника Уповноваженого з питань захисту персональних даних (надалі – Представник), а в структурі Секретаріату Уповноваженого створено Департамент з питань захисту персональних даних. Саме Представникові делеговано повноваження Уповноваженого ВРУ з прав людини у сфері захисту персональних даних. Вичерпний перелік таких повноважень викладено в статті 23 Закону[155].

Згідно зі статтею 11 Закону України "Про Уповноваженого Верховної Ради України з прав людини"[156] та Наказу Уповноваженого від 27.07.2012 № 7/8-12 "Про затвердження Положення про представників Уповноваженого Верховної Ради України з прав людини"[157] Представник Уповноваженого – посадова особа, якій делеговано визначені повноваження Уповноваженого.

Крім безпосередньо Уповноваженого, контрольними повноваженнями у сфері захисту персональних даних, згідно зі статтею 8 та 18 Закону, належить органам правосуддя. Відповідну судову практику проаналізовано в дальшому розділі цього посібника.

8.2. Порядок реалізації Уповноваженим контрольних повноважень щодо захисту персональних даних

Основна форма контрольної діяльності Уповноваженого, його Представника та працівників Секретаріату згідно зі статтею 23 Закону – проведення перевірок володільців та розпорядників персональних даних «на підставі звернень або з власної ініціативи». Як форми цих перевірок Закон визначає виїзні, безвиїзні, планові та позапланові[158]. Предметом таких перевірок повинно бути встановлення факту додержання або порушення володільцями та розпорядниками персональних даних вимог Конституції та законодавства України, підзаконних і розпорядчих актів органів влади, чинних міжнародних договорів, стороною яких стала Україна і які стосуються захисту персональних даних.

---

155 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

156 Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23.12.1997 р. № 776/97-ВР. *Відомості Верховної Ради України*. 1998. 13 трав. (№ 20).

157 Положення про представників Уповноваженого Верховної Ради України з прав людини : Затверджено Наказом Уповноваженого Верховної Ради України з прав людини від 26.07.2012 р. № 7/8-12. URL: https://zakon.rada.gov.ua/laws/show/v07_8715-12#Text (дата звернення: 23.05.2021).

158 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Якщо ж говорити про володільців та розпорядників персональних даних, чия діяльність може бути приводом для перевірок, то це поняття охоплює широке коло осіб. До них, відповідно до частини 2 статті 4 Закону, зараховуються «підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону»[159]. Як бачимо, це поняття охоплює і органи державної влади, чия діяльність у разі проведення перевірок ДСЗПД становила б конфлікт інтересів.

Порядок проведення Уповноваженим, його Представником та іншими визначеними Уповноваженим службовими особами перевірок додержання законодавства про захист персональних даних окремо визначено Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, який затверджено Наказом Уповноваженого від 08.01.14 № 1/2-14 (далі – Порядок)[160]. Права посадових осіб Секретаріату Уповноваженого щодо ведення контролю у сфері додержання законодавства про захист персональних даних, зокрема в ході проведення перевірок, визначено статтею 23 Закону та відповідними положеннями Порядку.

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**, невіддільну частину посвідчення, що підтверджує обсяг повноважень працівника Секретаріату.

Nota bene!

1. Посвідчення та додаток до нього – єдині документи, які працівник Секретаріату повинен мати при собі для проведення перевірки.
2. Володільцеві не надсилають ніяких попереджень щодо проведення перевірки працівниками Секретаріату.

У 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

159 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

160 Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: Затверджено Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення: 23.05.2021).

доступу до всіх приміщень, де проводиться обробка персональних даних. Єдина умова надання такого доступу – необхідність таких дій для ведення 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»[161].

Як невиконання законних вимог розцінюються такі 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 відповідні посадові особи Секретаріату Уповноваженого складають акт, у якому викладають інформацію щодо отриманих у ході перевірки документів та інформації, встановлених фактів, і висновки щодо наявності/або ні порушень законодавства про захист персональних даних.

Ключова ідея перевірок Уповноваженого в цій сфері – відновлення порушених прав громадян – суб'єктів персональних даних. Відповідно, на підставі вказаних висновків ухвалюється рішення щодо вжиття визначених Законом заходів реагування – винесення припису або за наявності складу адміністративного правопорушення, передбаченого статтею 188-39 Кодексу України про адміністративні правопорушення[162], складення адміністративного протоколу.

Мета винесення припису – припинення порушення законодавства про захист персональних даних та, по змозі, його виправлення, а також усунення

161 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. – К., 2014. – С. 298.

162 Кодекс України про адміністративні правопорушення : Закон України від 18 грудня 1984 р. *Відомості Верховної Ради УРСР.* 1984. № 40. Ст. 1122.

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 зрозумілі й окремого роз'яснення не потребують. Їх мета – припинити порушення Закону (наприклад, видалити дані, що обробляються незаконно), відновити порушені права (наприклад, надати суб'єктові доступ до його персональних даних чи змінити його персональні дані, що не відповідають дійсності) або запобігти потенційним порушенням у майбутньому (наприклад, припинити обробку (зокрема, збір, зберігання та використання) персональних даних, що не необхідні для досягнення задекларованої легітимної мети їх обробки, запровадити додаткові заходи захисту персональних даних).

Володілець або розпорядник, чия діяльність з обробки персональних даних була об'єктом перевірки, повинен усунути встановлене порушення протягом визначеного у приписі строку. Про вжиття відповідних заходів та припинення порушення вони зобов'язані письмово проінформувати Уповноваженого, а також надати копії документів, що підтверджують усунення порушень[163].

Nota bene!

Відповідно до статті 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»[164].

Виходячи з цього, слід наголосити, що акт складається лише за результатами проведення перевірки. Якщо за результатами розгляду звернення буде виявлене правопорушення, що не вимагатиме проведення перевірки (наприклад, для підтвердження факту такого правопорушення не потрібно отримувати додаткових матеріалів або достатньо отримати підтвердні документи чи пояснення сторін), працівники Секретаріату відразу винесуть припис/складуть протокол.

163 Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних : Затверджено Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення: 23.05.2021).

164 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Крім винесення припису, чинним законодавством передбачено можливість складати адміністративні протоколи за скоєння певних порушень законодавства про захист персональних даних[165]. Детальніше питання адміністративної та кримінальної відповідальності за порушення у сфері захисту персональних даних розглянуть у дальшому розділі посібника.

Детальну статистику контрольної діяльності Уповноваженого Верховної Ради з прав людини у сфері захисту персональних даних можна побачити в таблиці нижче.

	Отримані звернення	Проведені перевірки	Складені протоколи
2014[166]	928	53	8
2015[167]	638	62	3
2016[168]	1306	76	5
2017[169]	1211	45	34
2018[170]	806	41	14
2019[171]	1061	36	10
2020[172]	2031	67	9

Даних за 2018 рік у Щорічних звітах Уповноваженого, на жаль, нема. Як бачимо, у період пандемії відбулося різке зростання кількості звернень до Уповноваженого щодо порушень у сфері захисту персональних даних. Це може

---

165 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

166 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні. К., 2015. С. 225.

167 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. К., 2016. URL: https://ombudsman.gov.ua/files/Dopovidi/Dopovid_2016_final.pdf (дата звернення: 23.05.2021).

168 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. К., 2017. URL: https://ombudsman.gov.ua/files/Dopovidi/Dopovid_2017.pdf (дата звернення: 23.05.2021).

169 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. К., 2018. URL: https://ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf (дата звернення: 23.05.2021).

170 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. К., 2019. С. 81.

171 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. К., 2020. С. 194–199.

172 Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні. К., 2020. С. 21–28.

обумовлюватися кількома факторами: активнішим користуванням цифровими сервісами, у ході яких проводиться обробка персональних даних; обробкою медичних персональних даних значно більшими обсягами; активізацією інструментів цифрового та електронного маркетингу і реклами з боку бізнесу. Водночас кількість перевірок залишається на приблизно сталому рівні з 2014 року, а кількість складених протоколів, навпаки, має тенденцію до зниження.

За будь-яких обставин контрольні механізми у сфері захисту персональних даних – важливий інструмент забезпечення демократичних прав і свобод в умовах інформаційного суспільства. Їх значення зростає одночасно зі зростанням темпів цифровізації та в умовах пандемії, коли ростуть обсяги та ризики обробки персональних даних. Тому в найближчі періоди можна обґрунтовано чекати зростання кількості звернень до цих механізмів та їх активізації.

8.3. Проблеми та перспективи подальшого розвитку інституційного механізму контролю за додержанням законодавства у сфері захисту персональних даних

Модель контролю у сфері захисту персональних даних, яка існує в Україні, лише одна з можливих. Наприклад, у Франції контроль за додержанням законодавства у сфері захисту персональних даних веде колегіальний орган – *Національна комісія з питань інформатизації та свобод* (фр. *Commission nationale de l'informatique et des libertés*). Тут можна провести паралелі з ДСЗПД, однак ключова відмінність – у способі формування. ДСЗПД був повністю урядовим органом, інтегрованим у вертикаль виконавчої влади, тоді як комісія формується з представників французького парламенту та низки інших організацій, що забезпечує баланс при розгляді питань та ухваленні рішень, а законодавчо закріплений статус гарантує незалежність і безсторонність.

Інша можлива модель – створення органів у формі спеціальних посад уповноважених вести контроль за дотриманням стандартів щодо захисту персональних даних, аналогічно до парламентських уповноважених у сфері захисту прав людини. Це може бути єдиний такий орган на цілу державу або ж у федеральних державах – у кожному суб'єкті федерації (наприклад, у Німеччині такі уповноважені є в кожній федеральній землі).

З 2015 року в Україні точаться дискусії щодо створення такого спеціально уповноваженого органу – *Інформаційного комісара*, з відповідними стандартами незалежності свого формування та діяльності. Важливе в цьому аспекті те, що мандат такого органу повинен охоплювати як захист персональних даних, так і доступ до публічної інформації. Також цей орган повинен мати повноваження щодо видання обов'язкових приписів для запобігання або усунення порушень

права на доступ, отримувати доступ до інформації, зокрема з обмеженим доступом тощо[173].

Передання таких функцій обумовлено низкою причин. Наприклад, колишня Представниця Уповноваженого з прав людини щодо доступу до публічної інформації Ірина Кушнір зазначає, що така перевантаженість Секретаріату Уповноваженого та те, що у разі здійснення Уповноваженим контрольної функції щодо інформаційних прав громадян він не може гарантувати незалежність захисту цього права, якщо громадянин захоче оскаржити висновки Офісу Уповноваженого. Своєю чергою, тодішній Уповноважений Валерія Лутковська обґрунтовувала цю потребу низькою ефективністю приписів Уповноваженого та непритаманністю для національних інституцій із захисту прав людини функцій покарання за порушення[174].

Позицію щодо створення такої незалежної інституції підтримують і міжнародні експерти. Наприклад, Наташа Пірч Мусар підкреслювала, що «Перша і найважливіша рекомендація для України – створення незалежного (спеціального) інституту Інформаційного комісара або комісії, який має бути єдиним органом другої інстанції з розгляду звернень/скарг щодо порушення права на доступ до інформації»[175]. Ця позиція, об'єктивно, може бути застосована і до сфери захисту персональних даних.

Водночас висловлюється думка, що Секретаріат має зберегти свою роль у процесі контролю за додержанням законодавства у сфері інформаційних прав громадян. У концепції Секретаріату Уповноваженого під керівництвом Валерії Лутковської, навіть за умови створення інституту Інформаційного комісара, Уповноважений зберігав функції парламентського контролю в цій сфері[176].

Практичне впровадження цього можливе лише через внесення змін до ст. 101 Конституції України, яка тепер передбачає: «Парламентський контроль за додержанням конституційних прав і свобод людини і громадянина здійснює Уповноважений Верховної Ради України з прав людини»[177]. Цю статтю необхідно доповнити положеннями про те, що на відповідні сфери (захист

---

173 Інформаційний комісар: хто захищатиме доступ до інформації. URL: https://dostup.pravda.com.ua/stories/publications/informatsiinyi-komisar-khto-zakhyshchatyme-dostup-do-informatsii (Дата звернення: 20.05.2021).

174 Інформаційний комісар: хто захищатиме доступ до інформації. URL: https://dostup.pravda.com.ua/stories/publications/informatsiinyi-komisar-khto-zakhyshchatyme-dostup-do-informatsii (Дата звернення: 20.05.2021).

175 Пірч Мусар Н. Повноваження Уповноваженого Верховної Ради з прав людини та законодавство у сфері доступу до публічної інформації. Аналіз законодавства та рекомендації. Проект Ради Європи «Зміцнення свободи медіа і створення системи Суспільного мовлення в Україні», 15 серпня 2016 р. С. 110. (С. 97–116.)

176 Інформаційний комісар: хто захищатиме доступ до інформації. URL: https://dostup.pravda.com.ua/stories/publications/informatsiinyi-komisar-khto-zakhyshchatyme-dostup-do-informatsii (Дата звернення: 20.05.2021).

177 Конституція України із змінами від 28 червня 1996. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (Дата звернення: 20.05.2021).

персональних даних, доступ до публічної інформації та ін.) поширюється мандат Інформаційного комісара.

Такий алгоритм буде застосовний навіть у разі використання інших моделей, наприклад створення колегіального органу за прикладом Франції. Інакше ми знову опинимось у ситуації, аналогічній до становища із ДСЗПД у 2011–2013 рр., коли незалежність цього органу було об'єктом критики.

У будь-якому разі, процедура внесення змін до Конституції України тривала та передбачає необхідність зібрати 300 голосів народних депутатів України. Попри активні дискусії щодо цього питання у 2015–2017 рр., ця процедура не розпочалася в той період і відповідні пропозиції не розглядаються на цьому етапі теж. Повернення до цієї ідеї можливе з ухваленням нової редакції Закону «Про захист персональних даних», тому об'єктивно запуск інституту Інформаційного комісара чи іншого аналогічного органу можливий не раніше від 2023–2024 рр.

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

9.1. Загальні положення щодо передачі персональних даних

Питання передачі персональних даних третім особам одне з ключових у законодавстві про захист персональних даних, бо зазвичай найсерйозніші порушення Закону трапляються саме внаслідок неправомірної передачі. Саме передача чи оприлюднення чутливої чи іншої інформації про особу може завдати найбільшої шкоди її правам. Це порушення, як уже зазначено вище, може за певних умов передбачати притягнення до відповідальності.

Будь-яка дія, внаслідок якої треті особи тим чи іншим способом (через доступ/передачу/поширення/оприлюднення тощо) ознайомлюються з персональними даними суб'єкта, повинна проводитися за наявності однієї з підстав, передбачених статтями 7 та 11 Закону, відповідати принципам, викладеним у статті 6 Закону. Стаття 16 доволі чітко викладає **порядок** доступу третіх осіб до персональних даних у межах процедури «запит – відповідь».

Виходячи з указаних положень Закону, по-перше, будь-яка передача персональних даних повинна проводитися за згодою особи або на підставі закону (див. розділ щодо принципів обробки, а також частину першу статті 16 Закону за наявності підстав, передбачених його статтями 7 (щодо чутливих даних) та 11 (щодо решти персональних даних). Будь-які відступи від указаних положень допускаються лише за умов, передбачених статтею 25 Закону.

Практика застосування Закону Уповноваженим

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

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

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

Суд запитував медичну інформацію лише за період із 2010 до травня 2013 року. Тому в диспансеру не було підстав для надання решти інформації (за період з червня 2013 до грудня 2014 року).

За результатом дослідження зібраних матеріалів встановлено, що довідку, яку в подальшому направлено до суду, підготовлено та направлено за вказівкою керівниці диспансеру, яка і засвідчила її оригінальність своїм підписом. Такі дії керівниці диспансеру містили, на думку Уповноваженого, ознаки адміністративного правопорушення, передбаченого частиною четвертою статті 188-39 Кодексу України про адміністративні правопорушення, а саме **недодержання** встановленого законодавством про захист персональних даних **порядку захисту персональних даних**, що призвело до **незаконного доступу до них** та **порушення прав** заявника (як суб'єкта персональних даних), передбачених пунктом 7 частини другої статті 8 Закону.

У зв'язку з цим працівники Секретаріату Уповноваженого склали щодо керівниці диспансеру протокол про скоєння адміністративного правопорушення та направив його на розгляд та ухвалення рішення до суду.

Ще один важливий момент – вимоги щодо змісту запиту про передачу персональних даних. 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[178].

Ключовий елемент тут – необхідність зазначення мети/правових підстав для запиту, бо лише за цими відомостями володілець зможе ухвалити обґрунтоване рішення щодо доцільності передачі персональних даних. Ненадання в запиті відомостей щодо мети та підстав його направлення – формальна підстава для відмови в 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 підстав для надання персональних даних нема, відповідні працівники володільця будуть притягнуті до адміністративної відповідальності за частиною четвертою статті 188-39 КУПАП.

Практика застосування Закону Уповноваженим

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

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

Дослідження матеріалів вихідної кореспонденції засвідчило, що медичний заклад направив 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 незалежний володілець.

178 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

У ході перевірки досліджено також фактичні підстави передачі запитаної Департаментом інформації. Для цього проведено додаткову перевірку Департаменту, у 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 вело пошук грантових коштів.

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

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

Ще один проблемний аспект, пов'язаний з передачею персональних даних – ідентифікація особи отримувача. Зазвичай для того, щоб дістати 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 тощо), 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 розв'язувати такі питання (див. приклад щодо ідентифікації запитувача вище).

9.2. Правові стандарти транскордонної передачі персональних даних

Передача персональних даних між суб'єктами, володільцями та розпорядниками, які перебувають у різних державах стає дедалі актуальнішою в умовах цифрової економіки. Для України це питання особливо актуальне за структури економіки, у якій ІТ-сектор формує 4 % національного ВВП і третій за обсягом валютних надходжень. Його діяльність здебільшого пов'язана з експортом послуг українських фахівців, який може передбачати доступ до персональних даних громадян інших держав.

У Законі це питання врегульоване в статті 29, «Міжнародне співробітництво та передача персональних даних», частина третя якої встановлює, що «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»[179]. Перелік таких держав, які забезпечують належний захист, повинен визначати Кабінет Міністрів України.

У цій же статті передбачено, що «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»[180]. Закон встановлює і певні критерії щодо такої передачі, зокрема транскордонна передача персональних даних можлива лише з тією метою, з якою вони були зібрані, також у разі:

- надання суб'єктом персональних даних однозначної згоди на таку передачу;
- необхідності укладення чи виконання правочину між володільцем персональних даних та третьою особою – суб'єктом персональних даних на користь суб'єкта персональних даних;
- необхідності захисту життєво важливих інтересів суб'єктів персональних даних;
- необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги;
- надання володільцем персональних даних відповідних гарантій щодо невтручання в особисте і сімейне життя суб'єкта персональних даних[181].

---

179 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

180 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

181 Про захист персональних даних : Закон України від 01.07.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. 7 лип. (№ 122).

Якщо вести мову про передачу персональних даних до України, українським розпорядникам та володільцям, то воно, станом на 2021 рік, регламентується на трьох рівнях:

1) у рамках механізмів Конвенції 108 Ради Європи;

2) у рамках Регламенту ЄС;

3) у рамках внутрішнього законодавства окремих держав.

У першому випадку транскордонна передача персональних даних , згідно зі статтею 14 Конвенції 108+, можлива у разі наявності належних юридичних підстав, а саме:

- законодавства держави або міжнародної організації, куди передаються персональні дані, зокрема відповідні міжнародні договори або угоди; або ж якщо існують,
- спеціальних або затверджених стандартизованих гарантій, передбачених юридично зобов'язальними та придатними до виконання документами, прийнятими та реалізованими особами, які беруть участь у передачі та подальшій обробці[182].

Щодо ЄС, згідно зі статтею 45 Регламенту, передача персональних даних без обмежень можлива: «якщо [Європейська] Комісія вирішила, що третя країна, територія чи один або декілька визначених секторів у межах такої третьої країни, або відповідна міжнародна організація забезпечує належний рівень захисту»[183]. Такими державами, станом на сьогодні, Європейська Комісія визнала Андорру, Аргентину, Канаду (окремі види організацій), Фарерські острови, Гернсі, Острів Мен, Ізраїль, Джерсі, Нову Зеландію, Швейцарію та Уругвай. Передача персональних даних громадян та резидентів ЄС до США можлива в рамках спеціального режиму[184].

У разі якщо держава не визнана такою, то згідно зі статтею 46 Регламенту, володілець і розпорядник ЄС «можуть передавати персональні дані до третьої країни чи міжнародної організації, лише якщо контролер або оператор надав належні гарантії, та за умови наявності прав суб'єктів даних, що підлягають забезпеченню їхньої реалізації, та дієвих засобів правового захисту

182 Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data) of 18th May, 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Date of request: 2021).

183 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021).

184 Посібник з європейського права у сфері захисту персональних даних 2018. К.: К.І.С., 2020. С. 276–277.

для суб'єктів даних»[185]. Відповідні гарантій перелічені в цій статі. Українські суб'єкти відносин у сфері захисту персональних даних підпадають під дію саме цієї статті.

185 Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021).

10. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Важливість вказаного питання обумовлюється тим, що створення ефективної системи відповідальності за порушення законодавства про захист персональних даних один із ключових факторів, що здатні гарантувати дотримання його положень. Йдеться не лише про власне покарання порушників, а й про стримчий, превентивний ефект норм щодо відповідальності, якого можливо досягти лише за умови їх ефективної реалізації на практиці. Як уже зазначено вище, український Закон, попри численні недоліки, встановлює низку базових вимог щодо обробки персональних даних. Саме їх дотримання «суб'єктами відносин, пов'язаних із персональними даними», у розумінні ст. 4 Закону, повинне створити базу для подальшого розвитку законодавства про захист персональних даних та увідповіднення його чинним стандартам ЄС.

Ст. 28 Закону передбачено, що «порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом». Спеціальні положення щодо кримінальної та адміністративної відповідальності містяться у відповідних кодексах. Нижче проаналізовано ці положення детальніше.

10.1. Кримінальна відповідальність за порушення у сфері захисту персональних даних

Згідно зі ст. 182 («Порушення недоторканності приватного життя») Кримінального кодексу України, «Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, караються штрафом від п'ятисот до однієї тисячі неоподаткованих мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років. Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк[186].

186 Кримінальний кодекс України : Закон України від 5 квітня 2001 р. *Відомості Верховної Ради України.* 2001. № 25. Ст. 131.

Слід одразу зазначити, що практики застосування ст. 182 Кримінального кодексу України в Єдиному державному реєстрі судових рішень **практично нема**. Серед поодиноких рішень, ухвалених за цією статтею, можна назвати вироки у справах, предметом яких було незаконна передача конфіденційної інформації (персональних даних) володільцем третім особам[187] та незаконний збір та зберігання персональних даних[188].

Звісно, що такий стан справ може пояснюватися браком відповідних рішень у реєстрі чи проблемами пошуку, однак цілком можливо, і це видається правдоподібнішим поясненням, що цю статтю, справді, вкрай рідко застосовують національні органи влади. Отже, можна говорити про те, що це положення наразі фактично не діє.

10.2. Адміністративна відповідальність за порушення у сфері захисту персональних даних

Адміністративна відповідальність за порушення у сфері обробки та захисту персональних даних встановлена ст. 188-39 Кодексу України про адміністративні правопорушення (надалі – КупАП). Вказаним положенням передбачено відповідальність за:

1) 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;

2) 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;

3) 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.

---

187 Вирок Шевченківського районного суду міста Києва від 08 грудня 2014 року по справі № 761/29030/13-к. URL: https://reyestr.court.gov.ua/Review/42173797 (цит. 23.05.2021).

188 Вирок Баглейського районного суду Дніпродзержинська від 13 лютого 2013 р. по справі № 404/5528/12. URL: https://reyestr.court.gov.ua/Review/29396197 (цит. 23.05.2021); Вирок Придніпровського районного суду міста Черкаси від 29 квітня 2011 р. по справі №1-162/11. URL: https://reyestr.court.gov.ua/Review/49482456 (цит. 23.05.2021).

Також передбачена відповідальність і за повторне скоєння цих порушень. Щодо санкцій, то вони передбачають штраф розміром від ста до двох тисяч неоподатковуваних мінімумів доходів громадян.

Якщо вести мову про частину першу ст. 188-39 КУПАП, то обов'язок повідомляти Уповноваженого про обробку персональних даних передбачено ст. 9 Закону. Згідно з указаним положенням, володілець персональних даних повідомляє Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки. Такі види обробки визначив Уповноважений наказом від 8 січня 2014 року № 1/02-14, яким затверджено *Порядок повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації*. Станом на сьогодні нема випадків притягнення до адміністративної відповідальності за неповідомлення Уповноваженого. Повний брак правопорушень такого характеру вкрай малоймовірний. Отже, видається, що вказане положення КУпАП не працює на практиці.

Загалом же чч. 1 та 2 ст. 188-39 КУпАП доволі однозначні та чіткі й не потребують додаткових роз'яснень. Також слід зазначити, що вказаними положеннями передбачається відповідальність за порушення лише незначних аспектів законодавства про захист персональних даних. Здебільшого йдеться про порушення володільцями своїх зобов'язань перед Уповноваженим. Разом з тим жодне з вказаних положень не передбачає відповідальності за порушення правил обробки / захисту персональних даних. Однак саме відносини, пов'язані з обробкою та захистом персональних даних, і є ключовий предмет правового регулювання Закону.

У цій частині законодавець запровадив ч. 4 ст. 188-39 КУПАП. Вказаним положенням передбачено відповідальність за порушення, скоєні в ході власне обробки / захисту персональних даних. У зв'язку з цим, а також з огляду на деяку складність викладу вказаної частини ст. 188-39 КУПАП, видається необхідним детальніше її проаналізувати. З об'єктивної сторони вказане положення містить два елементи, пов'язані причиново-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.

Щодо першого, слід наголосити, що в законодавстві нема не лише означення понять **«захист персональних даних»** та **«порядок захисту персональних даних»**, а й будь-яких вимог щодо того, яким критеріям повинен відповідати такий захист. Єдине, що передбачено Законом в цій частині, – це обов'язок забезпечити «захист даних» (ст. 24 Закону).

Можна зробити припущення, що йдеться, **з одного боку,** про загальний обов'язок володільця вживати організаційних та технічних заходів з метою запобігання випадковій втраті або знищенню, незаконній обробці, зокрема незаконному знищенню чи доступові до персональних даних, **а з іншого** – про обов'язок кожного працівника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних, чи службових, чи трудових обов'язків.

Однак, перед тим як робити будь-які висновки щодо дії та ефективності тих чи інших положень законодавства, варто проаналізувати практику їх застосування. З огляду на практику, яка сформувалася за результатами розгляду судами протоколів про адміністративні порушення[189], можна стверджувати, що поняття «встановленого законодавством про захист персональних даних порядку захисту персональних даних» тлумачиться доволі широко та охоплює **будь-які дії, які становлять порушення Закону** (див. детальніше нижче). Загалом же тлумаченню цього поняття взагалі не приділяється уваги в рішеннях судів, зазвичай вони автоматично займають таку позицію.

Тому видається доцільним запровадити як у КУпАП, так і в Законі певні, хоча б базові вимоги щодо якості та рівня такого захисту (достатність/адекватність/пропорційність тощо), обов'язку вжити заходів для визначення необхідного

189 Постанова Дніпровського районного суду м. Києва від 15 квітня 2015 р. по справі № 755/3821/15-п URL: http://reyestr.court.gov.ua/Review/43778626 (цит. 26.01.2019); Постанова Дарницького районного суду м. Києва від 11 вересня 2015 р. по справі № 753/13021/15-п URL: http://reyestr.court.gov.ua/Review/50886437 (цит. 26.01.2019)'; Постанова Голосіївського районного суду м. Києва від 02 листопада 2015 р. по справі № 752/15256/15-п URL: http://reyestr.court.gov.ua/Review/53305602 (цит. 26.01.2019); Постанова Татарбунарського районного суду Одеської області від 09 липня 2018 р. по справі № 515/952/18 URL: http://reyestr.court.gov.ua/Review/75208254 (цит. 26.01.2019); Постанова Жовтневого районного суду міста Маріуполя від 11 травня 2018 р. по справі № 263/4314/18 URL: http://reyestr.court.gov.ua/Review/73915418 (цит. 26.01.2019); Постанова Подільського районного суду міста Києва від 29 грудня 2018 р. по справі № 758/4389/17 URL: http://reyestr.court.gov.ua/Review/71400435 (цит. 26.01.2019); Постанова Городищенського районного суду Черкаської області від 27 листопада 2018 р. по справі № 691/1261/17. URL: http://reyestr.court.gov.ua/Review/70667984 (цит. 26.01.2019); Постанова Івано-Франківського міського суду Івано-Франківської області від 26 вересня 2018 р. по справі № 344/8443/17. URL: http://reyestr.court.gov.ua/Review/70072924 (цит. 26.01.2019); Постанова Жовтневого районного суду міста Дніпропетровська від 14 вересня 2017 р. по справі № 201/12780/17-п. URL: http://reyestr.court.gov.ua/Review/68948324 (цит. 26.01.2019); Постанова Коломийського міськрайонного суду Івано-Франківської області від 14 лютого 2017 р. по справі № 346/200/17. URL: http://reyestr.court.gov.ua/Review/64723526 (цит. 26.01.2019); Постанова Галицького районного суду Львівської області від 03 квітня 2017 р. по справі №461/2021/17. URL: http://www.reyestr.court.gov.ua/Review/65734627 (цит. 26.01.2019); Постанова Московського районного суду міста Харкова від 04 травня2017 р. по справі №643/3384/17. URL: http://reyestr.court.gov.ua/Review/66441353 (цит. 26.01.2019); Постанова Оболонського районного суду міста Києва від 19 жовтня 2016 р. по справі №756/11255/16-п. URL: http://reyestr.court.gov.ua/Review/62225162 (цит. 26.01.2019).

рівня захисту (проводити діагностику систем захисту, визначення ризиків, пов'язаних з обробкою тощо) та інше.

Далі, згідно з КупАП, для того щоб становити порушення ст. 188-39, такі дії повинні бути в причиново-наслідковому зв'язку з 1) незаконним доступом до персональних даних або 2) порушенням прав суб'єкта персональних даних.

З незаконним доступом усе більш-менш зрозуміло, наприклад порушення порядку захисту, що призвело до незаконного доступу третіх осіб. Разом з тим варто ще раз наголосити на важливому понятійному аспекті. Традиційно (зокрема, в Регламенті та Конвенції) під доступом (*access*) розуміється власне доступ суб'єкта до своїх персональних даних. Згідно ж зі ст. 16 Закону, під доступом до персональних даних розуміється як доступ суб'єкта до своїх персональних даних, так і доступ до його персональних даних третіх осіб, що однак відбувається в порядку «запит-відповідь». Доцільність такого вибору термінології, як і самого механізму, передбаченого ст. 16 Конвенції, викликають сумнів. Зараз важливо лише те, що сама конструкція притягнення до відповідальності більш-менш зрозуміла.

З іншою частиною структури ч. 4 ст. 189-39 КУпАП ситуація дещо складніша. Формулювання «*захист прав суб'єкта персональних даних*» автоматично відсилає до ст. 8 Закону («Права суб'єкта персональних даних»). У вказаному положенні йдеться, серед іншого, про право отримувати інформацію про те, які дані, як та ким обробляються; заперечувати проти обробки; відкликати згоду на обробку персональних даних; звертатися зі скаргами на незаконну обробку; та право на захист від незаконної обробки, пошкодження, поширення неправдивих даних та прийняття автоматизованого рішення.

Однак на практиці важко уявити порушення «*порядку захисту персональних даних*», що призвело б до порушення права «*отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані*», права «*знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки*» чи, наприклад, права «*на захист від автоматизованого рішення, яке має для нього правові наслідки*» (пп. 2, 3 та 13 частини другої ст. 8 Закону) та ін.[190]. Вказані комбінації виглядають позбавленими будь-якого змісту.

Єдине змістовне поєднання (і то лише частково), яке випливає з положень вказаної статті це недодержання «*порядку захисту персональних даних*», 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» (ст. 8 Закону).

---

190 Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI. *Офіційний вісник України.* 2010. № 49. Ст. 1604.

У сферу дії вказаного положення КУпАП очевидно потрапляють дії, пов'язані з незаконною передачею, розкриттям, втратою, знищенням та зміною персональних даних, **якщо** вони були спричинені недодержанням «*встановленого законодавством про захист персональних даних порядку захисту персональних даних*».

На практиці ж у сферу дії вказаної статті потрапляє здебільшого незаконна передача персональних даних (чи незаконний доступ з боку третіх осіб)[191]. Здебільшого осіб притягують до відповідальності на підставі частини четвертої ст. 188-39 КУПАП за незаконну передачу персональних даних третім особам у разі:

- вивішування списків осіб, які звернулися по отримання адміністративних послуг, центром надання адміністративних послуг[192];
- поширення медичним закладом інформації щодо стану психічного здоров'я[193];

---

191 Постанова Дніпровського районного суду м. Києва від 15 квітня 2015 р. по справі № 755/3821/15-п URL: http://reyestr.court.gov.ua/Review/43778626 (цит. 26.01.2019); Постанова Дарницького районного суду м. Києва від 11 вересня 2015 р. по справі № 753/13021/15-п URL: http://reyestr.court.gov.ua/Review/50886437 (цит. 26.01.2019)'; Постанова Голосіївського районного суду м. Києва від 02 листопада 2015 р. по справі № 752/15256/15-п URL: http://reyestr.court.gov.ua/Review/53305602 (цит. 26.01.2019); Постанова Татарбунарського районного суду Одеської області від 09 липня 2018 р. по справі № 515/952/18 URL: http://reyestr.court.gov.ua/Review/75208254 (цит. 26.01.2019); Постанова Жовтневого районного суду міста Маріуполя від 11 травня 2018 р. по справі № 263/4314/18 URL: http://reyestr.court.gov.ua/Review/73915418 (цит. 26.01.2019); Постанова Подільського районного суду міста Києва від 29 грудня 2018 р. по справі № 758/4389/17 URL: http://reyestr.court.gov.ua/Review/71400435 (цит. 26.01.2019); Постанова Городищенського районного суду Черкаської області від 27 листопада 2018 р. по справі № 691/1261/17. URL: http://reyestr.court.gov.ua/Review/70667984 (цит. 26.01.2019); Постанова Івано-Франківського міського суду Івано-Франківської області від 26 вересня 2018 р. по справі № 344/8443/17. URL: http://reyestr.court.gov.ua/Review/70072924 (цит. 26.01.2019); Постанова Жовтневого районного суду міста Дніпропетровська від 14 вересня 2017 р. по справі № 201/12780/17-п. URL: http://reyestr.court.gov.ua/Review/68948324 (цит. 26.01.2019); Постанова Коломийського міськрайонного суду Івано-Франківської області від 14 лютого 2017 р. по справі № 346/200/17. URL: http://reyestr.court.gov.ua/Review/64723526 (цит. 26.01.2019); Постанова Галицького районного суду Львівської області від від 03 квітня 2017 р. по справі №461/2021/17. URL: http://www.reyestr.court.gov.ua/Review/65734627 (цит. 26.01.2019); Постанова Московського районного суду міста Харкова від від 04 травня 2017 р. по справі №643/3384/17. URL: http://reyestr.court.gov.ua/Review/66441353 (цит. 26.01.2019); Постанова Оболонського районного суду міста Києва від 19 жовтня 2016 р. по справі №756/11255/16-п. URL: http://reyestr.court.gov.ua/Review/62225162 (цит. 26.01.2019).

192 Постанова Дніпровського районного суду м. Києва від від 15 квітня 2015 р. по справі № 755/3821/15-п URL: http://reyestr.court.gov.ua/Review/43778626 (цит. 26.01.2019); Постанова Ковпаківського районного суду м. Суми від 07 липня 2015 р., провадження № 3/592/1440/15. URL: http://reyestr.court.gov.ua/Review/46341181 (цит. 26.01.2019).

193 Постанова Ковпаківського районного суду м. Суми від від 07 липня 2015 р., провадження № 3/592/1440/15. URL: http://reyestr.court.gov.ua/Review/46341181 (цит. 26.01.2019).

- вивішування списку боржників ОСББ, гуртожитками чи садовими товариствами[194] чи поширення такої інформації в інтернеті[195];
- поширення ОСББ даних внутрішньо переміщених осіб[196]; оприлюднення персональних даних посадовими особами державних установ[197] чи юридичних осіб[198] в інтернеті;

194 Постанова Дарницького районного суду м. Києва від 11 вересня 2015 р. по справі № 753/13021/15-п URL: http://reyestr.court.gov.ua/Review/50886437 (цит. 26.01.2019); Постанова Голосіївського районного суду м. Києва від 02 листопада 2015 р. по справі № 752/15256/15-п URL: http://reyestr.court.gov.ua/Review/53305602 (цит. 26.01.2019); Постанова Жовтневого районного суду міста Маріполя від 11 травня 2018 р. по справі № 263/4314/18 URL: http://reyestr.court.gov.ua/Review/73915418 (цит. 26.01.2019); Постанова Оболонського районного суду міста Києва від 19 жовтня 2016 р. по справі №756/11255/16-п. URL: http://reyestr.court.gov.ua/Review/62225162 (цит. 26.01.2019); Постанова Суворовського районного суду міста Одеси від 24 грудня 2020 р. по справі № 523/16653/20. URL : https://reyestr.court.gov.ua/Review/93870287 (цит. 04.04.2021); Постанова Ленінського районного суду м.Запоріжжя по справі № 334/4896/20 від 23 вересня 2020 р. URL: https://reyestr.court.gov.ua/Review/91766936 (Цит. 04.04.2021); Постанова Броварського міськрайонного суду Київської області по справі 361/1579/20 від 09 квітня 2020 р. URL: https://reyestr.court.gov.ua/Review/88698313 (цит. 04.04.2021).

195 Постанова Апеляційного суду Київської області від 07 квітня 2016 р. по справі №369/1458/17. URL: http://reyestr.court.gov.ua/Review/65897756 (цит. 26.01.2019); Постанова Києво-Святошинського районного суду Київської області від 02 березня 2017 р. по справі №369/1458/17. URL: http://reyestr.court.gov.ua/Review/65897756 (цит. 26.01.2019); Постанова Жовтневого районного суду м. Маріуполя Донецької області по справі № 263/9809/20 від 19 серпня 2020 р. URL : https://reyestr.court.gov.ua/Review/91050985 (Цит. 04.04.2021); Постанова Хортицького районного суду м.Запоріжжя по справі №337/3876/20 від 30 жовтня 2020 р. URL: https://reyestr.court.gov.ua/Review/92657926 (Цит. 04.04.2021); Постанова Ленінського районного суду м. Запоріжжя по справі № 334/3379/20 від 15 липня 2020 р. URL : https://reyestr.court.gov.ua/Review/90599358. (Цит. 04.04.2021); Постанова Нетішинського міського суду Хмельницької області по справі № 679/1676/19 від 09 грудня 2019 р. URL: https://reyestr.court.gov.ua/Review/86237026 (Цит. 04.04.2021).

196 Постанова Апеляційного суду Луганської області від від 08 листопада 2016 р. по справі № 369/1458/17. URL: http://reyestr.court.gov.ua/Review/62541147 (цит. 26.01.2019).

197 Постанова Татарбунарського районного суду Одеської області від 09 липня 2018 р. по справі № 515/952/18. URL: http://reyestr.court.gov.ua/Review/75208254 (цит. 26.01.2019); Постанова Соснівського районного суду м. Черкаси по справі № 712/7293/19 від 04 липня 2019 р. URL: https://reyestr.court.gov.ua/Review/82822611. (Цит. 04.04.2021); Постанова Коломийського міськрайонного суду Івано-Франківської області по справі № 346/5963/19 від 13 березня 2020 р. URL: https://reyestr.court.gov.ua/Review/88214446 (Цит. 04.04.2021).

198 Постанова Жовтневого районного суду міста Дніпропетровська від 14 вересня 2017 р. по справі № 201/12780/17-п. URL: http://reyestr.court.gov.ua/Review/68948324 (цит. 26.01.2019); Постанова Жовтневого районного суду міста Маріуполя Донецької області по справі 263/16968/19 від 27 листопада 2019 р. URL: https://reyestr.court.gov.ua/Review/85946057 (Цит. 04.04.2021); Постанова Жовтневого районного суду м. Маріуполя по справі № 263/3810/19 від 08 травня 2019 р. URL : https://reyestr.court.gov.ua/Review/81590161 (Цит. 04.04.2021); Постанова Вишгородського районного суду Київської області по справі № 363/4644/20 від 21 січня 2021 р. URL: https://reyestr.court.gov.ua/Review/94316421 (Цит. 04.04.2021).

- незаконної передачі органом державної влади чи саморегулівної організації частини державної бази персональних даних[199];
- оприлюднення військовим комісаріатом списків призовників[200];
- передачі третім особам персональних даних державним органом влади чи саморегулівною організацією[201].

Отже, попри широкий, на перший погляд, характер вказаного положення, сфера його дії доволі вузька. Натомість, самі по собі порушення окремих найвагоміших положень Закону **можуть (і повинні) кваліфікуватись як окремі правопорушення у сфері законодавства про захист персональних даних**. Як приклад, можна навести:

- неповідомлення суб'єкта про збір персональних даних,
- незаконну обробку (і зокрема поширення) персональних даних, яка не пов'язана з порушенням порядку захисту,
- 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'єктові 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,
- брак 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.

Станом на сьогодні виявлення таких порушень зазвичай завершується винесенням припису Уповноваженого, мета якого – їх усунення. У приписі можуть

---

199 Постанова Подільського районного суду міста Києва від 29 грудня 2018 р. по справі № 758/4389/17. URL: http://reyestr.court.gov.ua/Review/71400435 (цит. 26.01.2019); Постанова Подільського районного суду м. Києва по справі № 758/14158/19 від 07 лютого 2020 р. URL: https://reyestr.court.gov.ua/Review/87632133 (Цит. 04.04.2021).

200 Постанова Городищенського районного суду Черкаської області від 27 листопада 2018 р. по справі № 691/1261/17. URL: http://reyestr.court.gov.ua/Review/70667984 (цит. 26.01.2019); Постанова Коломийського міськрайонного суду Івано-Франківської області по справі № 346/5287/20 віж 23 грудня 2020 р. по справі № 346/5287/20.

201 Постанова Галицького районного суду Львівської області від 03 квітня 2017 р. по справі №461/2021/17. URL: http://www.reyestr.court.gov.ua/Review/65734627 (цит. 26.01.2019).

бути висунуті будь-які вимоги, необхідні для вдосконалення системи захисту персональних даних володільця/розпорядника[202]. Невиконання такого припису тягне за собою відповідальність, передбачену ч. 2 ст. 188-39 КУПАП (див. вище). Процедура функціонує так: 1) представники Уповноваженого проводять перевірку, 2) виявляють порушення, 3) виносять припис про його виправлення, і 4) лише в разі невиконання припису складають відповідний протокол про порушення частини другої ст. 188-39 КУПАП[203].

На перший погляд, усе видається логічним, однак на практиці така система неефективна. Володілець від самого початку незацікавлений у налагодженні належної системи захисту персональних даних. Як продемонстровано вище, хоч би яке серйозне порушення законодавства про захист персональних даних скоїв володілець, його можна притягнути до адміністративної відповідальності лише у разі, якщо це призвело до незаконного поширення персональних даних суб'єкта або порушення порядку доступу до них, визначеного ст. 16 Закону[204]. Теоретично володільця можна притягнути до відповідальності також у разі незаконного знищення, зміни чи втрати даних, однак жодної практики з цього приводу не виявлено. Інакше ж володільцеві загрожує лише винесення припису.

Отже, володільцеві/розпорядникові набагато зручніше дочекатися приходу з перевіркою наглядового органу (наприклад, за скаргою суб'єкта) та виконати винесений припис. Така ситуація підсилюється і тим, що, з огляду на обмежені ресурси Секретаріату Уповноваженого, ймовірність проведення такої перевірки, коли нема скарги, вкрай незначна.

Як наслідок, створюється також надмірне навантаження на наглядовий орган – Уповноваженого та Секретаріат Уповноваженого. Кожна перевірка працівників Секретаріату, в ході якої було виявлене правопорушення, повинна не лише мати наслідки для володільця-об'єкта перевірки, а й стримчий ефект щодо інших володільців. За чинної системи цього немає.

Тому видається доцільним ввести адміністративну відповідальність (нехай і незначну) за порушення окремих положень Закону без їх прив'язки до додаткових умов, як-от «*недодержання порядку захисту персональних даних*». Разом з тим слід визнати, що така система працюватиме, лише якщо відповідні положення Закону, порушення яких передбачає притягнення до адміністративної

---

202 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». *(Прим. авт.)*.

203 Постанова Івано-Франківського міського суду Івано-Франківської області від 26 вересня 2018 р. по справі № 344/8443/17. URL: http://reyestr.court.gov.ua/Review/70072924 (цит. 26.01.2019); Постанова Золочівського районного суду Львівської області від 20 грудня 2016 р. по справі 445/2022/16-п. URL: http://reyestr.court.gov.ua/Review/63869054 (цит. 26.01.2019).

204 Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI. *Офіційний вісник України*. 2010. № 49. Ст. 1604.

відповідальності, будуть достатньо чіткі та передбачувані. Наразі, як видно з попередніх розділів, це можна сказати далеко не про всі положення Закону. Отже, необхідно передовсім деталізувати відповідні положення Закону, а вже після цього вводити відповідальність за їх порушення.

Декілька інших факторів ще глибше ускладнюють такий стан справ і сприяють байдужому ставленню до положень Закону з боку володільців.

Аналізуючи вказані рішення національних судів, ми зауважили, що навіть у тих справах, де особу визнано винуватою у скоєнні адміністративного правопорушення, передбаченого ст. 188-39 КУпАП, суди не накладали стягнень і закривали провадження у зв'язку із закінченням строку їх накладення. Наприклад, відповідно до ч. 2 ст. 38 КУпАП стягнення може бути накладене не пізніш як через 3 місяці з дня скоєння адміністративного правопорушення, а при триванні правопорушення – не пізніш як через три місяці з дня його виявлення[205]. Цей строк загальний для великої кількості правопорушень, передбачених КУпАП. Однак аналіз практики засвідчує, що в абсолютній більшості випадків, він недостатній для вчасного оформлення адміністративного матеріалу, направлення його до суду та розгляду справи судом[206].

Видається, що основна перешкода для вчасного накладення стягнення – природа порушень законодавства про захист персональних даних. На відміну від порушень, які фіксують контрольні органи в момент їх виявлення та відразу передають до суду (порушення правил дорожнього руху, порушення митних правил тощо), порушення законодавства про захист персональних даних фіксують зазвичай у ході проведення перевірки за скаргами суб'єктів персональних даних, тобто коли порушення вже могло відбутися достатньо тривалий час тому. Це, зокрема, підтверджують проаналізовані вище рішення судів. Як наслідок, з моменту скоєння правопорушення та його виявлення суб'єктом до направлення справи до суду проходить досить значний час.

Більшість суб'єктів природно можуть намагатися розв'язати питання щодо усунення порушення шляхом самостійного звернення до володільця / розпорядника. Такий підхід загальноприйнятий і саме на цьому і базується система захисту персональних даних більшості держав. Підтвердження того – широкий набір інструментів, передбачених законодавством, зокрема ст. 8 («Права суб'єкта персональних даних») Закону. Згідно з указаним положенням Закону, суб'єкт має право вимагати видалення, зміни чи знищення своїх персональних даних чи направляти заперечення проти їх обробки.

---

205 Кодекс України про адміністративні правопорушення: Закон України від 18 грудня 1984 р. Відомості Верховної Ради УРСР. 1984. № 40. Ст. 1122.

206 Постанова Московського районного суду міста Харкова від 04 травня2017 р. по справі №643/3384/17. URL: http://reyestr.court.gov.ua/Review/66441353 (цит. 26.01.2019); Постанова Золочівського районного суду Львівської області від 20 грудня 2016 р. по справі 445/2022/16-п. URL: http://reyestr.court.gov.ua/Review/63869054 (цит. 26.01.2019).

Ба більше, контакт з володільцем часто необхідний також для того, щоб отримати докази порушення права. Незалежно від того, чи суб'єкт планує в подальшому звертатися до суду чи Уповноваженого йому необхідно належним чином обґрунтувати свою скаргу або позов, що здебільшого неможливо без звернення до володільця.

Далі, після того як суб'єкт направляє скаргу до офісу Уповноваженого, її розгляд також займає значний час. У цьому зв'язку слід звернути увагу на те, що Секретаріат Уповноваженого, працівники якого і займаються питаннями захисту персональних даних, працюють у Києві, а порушення трапляються в різних регіонах. Своєю чергою, регіональні представники Уповноваженого займаються всім колом питань і не завжди мають можливість та достатню кваліфікацію для проведення перевірки за скаргами про порушення законодавства про захист персональних даних. Фіксація факту порушення законодавства про захист персональних даних потребуватиме проведення перевірки (виїзної – у форматі перевірки чи безвиїзної – через направлення запитів), яка, також потребуватиме значних затрат часу.

І всі ці стадії можуть супроводжуватися значними затримками: надання відповідей в останній момент, надання нечітких і неповних відповідей, ненадання відповіді, перешкоджання в проведенні перевірки, за що штраф істотно менший, ніж за порушення законодавства про захист персональних даних[207].

Тому, навіть за умови швидкого проходження попередньої стадії, суддя може не встигнути розглянути матеріали про адміністративне правопорушення, не кажучи вже про те, що 1) матеріали можуть бути повернуті для увідповіднення їх процесуальним вимогам, 2) особа, на яку накладають стягнення, може затягувати розгляд справи, зловживаючи своїми процесуальними правами, а 3) суддя може бути перевантаженим роботою.

Тож видається необхідним вдосконалити чинні положення законодавства України щодо відповідальності за порушення про захист персональних даних. Зокрема, необхідно продовжити визначені законодавством строки накладення адміністративного стягнення за порушення законодавства про захист персональних даних і гарантувати ефективну діяльність контрольного органу як кількісно, так і через представництво в регіонах.

Як один із варіантів розв'язання вказаної проблеми можна також розглядати і можливість передачі повноважень щодо ухвалення рішення про накладення стягнення у зв'язку порушенням законодавства про захист персональних даних Уповноваженому.

У цьому зв'язку постає ще одна важлива проблема, а саме про доцільність поєднання Уповноваженим несумісних функцій парламентського контролю за

207 Таке порушення тягне за собою відповідальність відповідно до ст. 188-40 КУпАП («Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини») у вигляді штрафу розміром від ста до двохсот неоподатковуваних мінімумів доходів громадян. (Прим. авт.)

додержанням прав людини та контролю за додержанням законодавства про захист персональних даних. Видається, що повноваження з контролю за додержанням законодавства про захист персональних даних необхідно покласти на окрему інституцію (наприклад, на інформаційного комісара, спеціальну комісію тощо), як це і є в більшості держав – учасниць Конвенції № 108.

Окремо слід наголосити на необхідності вдосконалення положень щодо суб'єктного складу осіб, які можуть нести відповідальність за порушення законодавства про захист персональних даних. А що не завжди можливо встановити конкретну особу, відповідальну за порушення законодавства про захист персональних даних (навіть якщо з матеріалів справи очевидно, що поширення персональних даних скоїв хтось із працівників організації – володільця відповідних персональних даних[208]), то в такому разі повинна існувати можливість притягнення до відповідальності конкретної юридичної особи.

Підсумовуючи, можна констатувати, що протягом усього шляху розвитку українського законодавства про захист персональних даних його орієнтирами були саме європейські стандарти, які містяться в документах і міжнародних договорах Ради Європи та ЄС. Водночас у чинному законодавстві України про захист персональних даних міститься ціла низка прогалин і розбіжностей. Особливо показова, у цьому контексті ситуація з положеннями законодавства України, які регламентують питання відповідальності за порушення стандартів захисту персональних даних. До основних проблем, які існують у зв'язку з цим, можна віднести:

1) брак у законодавстві України повноцінного означення поняття «захист персональних даних» / критеріїв, яким повинен відповідати такий захист / вимог щодо визначення володільцем і розпорядником рівня такого захисту;

2) розмитість фактичних підстав відповідальності за порушення в ході обробки персональних даних;

3) недостатність винятково адміністративного стягнення як засобу покарання за порушення стандартів захисту персональних даних;

4) значні недоліки в процедурі накладення стягнення за скоєння адміністративного правопорушення, передбаченого ч. 4 ст. 188-39 КУпАП;

5) неефективність інституційної системи притягнення до відповідальності за порушення положень законодавства щодо захисту персональних даних, що наразі виконує Секретаріат Уповноваженого.

208 Постанова Жовтоводського міського суду Дніпропетровської області від 31 жовтня 2016 р. у справі 176/2309/16-п. URL: http://reyestr.court.gov.ua/Review/62786003 (цит. 26.01.2019).

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

- «Avilkina and Others v. Russia» (заява № 1585/09, рішення від 06/06/2013) – збір медичної інформації органами прокуратури в рамках перевірки. Законодавча невизначеність повноважень щодо збору інформації про особу. Надмірний обсяг зібраної інформації.
- «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.
- «Friedl v. Austria» (заява № 15225/89, рішення від 31/01/1995) – законність проведення відеофіксації силового розпуску мирного зібрання.
- «Gardel v. France» (заява № 16428/05, рішення від 17/12/2009) – ведення національними органами влади реєстру осіб, які скоїли злочини статевого характеру.
- «Garnaga v. Ukraine» (заява № 20390/07, рішення від 16/05/2013) – закріплена на законодавчому рівні неможливість змінити по батькові особи.
- «Gaskin v. The United Kingdom» (заява № 10454/83, рішення від 07/07/1989) – обмеження доступу особи до частини документів щодо її виховання опікуном/прийомними батьками. Відсутність незалежного органу, який би розглядав клопотання щодо надання доступу до частини вказаних документів.
- «I. v. Finland» (заява № 20511/03, рішення від 17/07/2008) – брак обліку операцій щодо надання доступу до медичної документації заявниці, що призвело до неможливості встановлення особи, яка, ймовірно, поширила інформацію, що містилася у ній.
- «Kennedy v. The United Kingdom» (заява № 26839/05, рішення від 18/05/2010); «Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria» (заява № 62540/00, рішення від 28/06/2007); «Klass and Others v. Germany « (рішення від 06/09/1978) – функціонування системи негласного спостереження правоохоронними органами.

- «K. H. and Others v. Slovakia» (заява № 32881/04, рішення від 06/11/2009) – ненадання лікарнею заявникам копій їхньої медичної документації.
- «Leander v. Sweden» (заява № 9248/81) – законність ведення таємного реєстру поліції та проведення перевірки особи за наявною в ньому інформацією перед зайняттям посади, що передбачала надання доступу до приміщень з обмеженим доступом. Законність ведення реєстру та отримання доступу до нього. Контроль за веденням реєстру.
- «L. H. v. Latvia» (заява № 52019/07, рішення від 29/04/2014) – збір контрольним органом інформації щодо стану здоров'я особи з метою оцінення якості наданої їй лікарнею медичної допомоги. Брак легітимної мети збору персональних даних. Надмірний обсяг зібраної інформації. Неврахування інтересів пацієнта.
- «L. L. v. France» (no. 7508/02, ECHR 2006-XI) – використання судом як доказів у справі про розлучення документів, що містили відомості про стан здоров'я. Суд вказав, що в цій справі використання вказаних доказів не було необхідним.
- «M. K. v. France» (заява № 19522/09, рішення від 18/04/2013) – ведення реєстру відбитків пальців.
- «M. S. v. Sweden» (заява № 34209/92, рішення від 27/08/1997) – передача лікарнею медичної інформації про особу на запит державного органу.
- «Peck v. The United Kingdom» (заява № 44647/98, рішення від 28/01/2003) – доцільність оприлюднення відеозапису, на якому видно особу після того, як вона намагалася скоїти самогубство;
- «P. G. and J. H. v. The United Kingdom» (заява № 44787/98, рішення від 25/09/2001) – добір, збереження та використання в ході судового провадження зразків голосу особи.
- «Rotaru v. Romania» (заява № 28341/95, рішення від 04/05/2000) – законність ведення службою безпеки таємного реєстру. Брак законодавчих гарантій.
- «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. Не було необхідності у зборі таких даних, якщо порівняти з отримуваними перевагами, неврахування індивідуальних обставин осіб, чиї дані зберігалися.
- «Shimovolos v. Russia» (заява № 30194/09, рішення від 21/06/2011) – законність функціонування таємного реєстру осіб, імовірно, причетних до екстремістської діяльності.

- «Uzun v. Germany» (заява № 35623/05, рішення від 02/09/2010) – спостереження за шляхами пересування особи (GPS-дані) відбувалося законно та було пропорційне. Не було порушення.
- «Z. v. Finland» (заява № 22009/93, рішення від 25/02/1997) – розкриття чутливої інформації в рішенні суду. Недостатність строків, впродовж яких обмежувався доступ до рішення суду, що містив таку інформацію.
- «Zaichenko v. Ukraine» (No. 2) (заява №45797/09, рішення від 26/02/2015) – брак визначеної законодавством процедури збору інформації під час проведення експертизи стану психіатричного здоров'я особи в межах провадження у справі про адміністративне правопорушення.

ДОДАТОК 2.
КЛЮЧОВІ РЕКОМЕНДАЦІЇ КОМІТЕТУ МІНІСТРІВ РАДИ ЄВРОПИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

- Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems;
- Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data;
- Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfill the rights of the child in the digital environment;
- Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries;
- Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests;
- Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality;
- Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment;
- Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users;
- Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services;
- Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines;
- Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010);
- Recommendation No.R(2002) 9 on the protection of personal data collected and processed for insurance purposes;

- Recommendation No.R(99) 5 for the protection of privacy on the Internet;
- Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes;
- Recommendation No.R(97) 5 on the protection of medical data;
- Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services;
- Recommendation No.R(92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system;
- Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies;
- Recommendation No.R(90) 19 on the protection of personal data used for payment and other related operations;
- Recommendation No.R(87) 15 regulating the use of personal data in the police sector;
- Recommendation No.R(86) 1 on the protection of personal data for social security purposes;
- Recommendation No.R(85) 20 on the protection of personal data used for the purposes of direct marketing;
- Resolution 29 on the protection of individuals vis-à-vis electronic data banks in the public sector (1974);
- Resolution 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector (1973).

ДОДАТОК 3.
ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Поняття «персональні дані», його нормативне означення.
2. Джерела правового регулювання захисту персональних даних: міжнародні та національні нормативно-правові акти.
3. Закон України «Про захист персональних даних» як основний.
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 для історичних, наукових та статистичних цілей відповідно до принципу визначеності мети обробки.
16. Принцип адекватності, ненадмірності та пропорційності обробки персональних даних.
17. Принцип вірогідності та точності обробки персональних даних.
18. Принцип чесності обробки персональних даних.
19. Інші принципи обробки персональних даних (підзвітності тощо).
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 із законом?
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'єктові 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 «вмотивованості вимоги» щодо статусу їх 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 конфіденційна інформація 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 стосовно 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 ведеться автоматизована обробка.

50. Зміст захисту персональних даних за замовчуванням (*privacy by default)*.

51. Статус осіб і 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 їхнім володільцем.

57. Порядок обліку операції, які проводяться з персональними даними з боку їх володільця.

58. Особливості обробки персональних даних володільцем – 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 повідомляти 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 ведення контролю за додержанням законодавства про захист персональних даних.

64. Положення законодавства України з ведення 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 світової та європейської системи захисту персональних даних.

72. Зміст нового Загального регламенту ЄС щодо захисту персональних даних.

73. Основні новели положень Конвенції №108+ (оновленої).

74. Судова практика щодо кримінальної відповідальності за порушення у сфері захисту персональних даних в Україні.

75. Судова практика щодо адміністративної відповідальності за порушення у сфері захисту персональних даних в Україні.

76. Основні проблеми відповідності чинного законодавства щодо захисту персональних даних України до Загального регламенту ЄС щодо захисту персональних даних.

77. Правові засади транскордонної передачі персональних з та в Україну.

78. Основні недоліки та прогалини чинного законодавства щодо захисту персональних даних в Україні.

79. Тенденції практики Секретаріату Уповноваженого Верховної Ради з прав людини в сфері захисту прав людини.

ДОДАТОК 4.
ПЕРЕЛІК ДЖЕРЕЛ

A. Спеціальна література

1. Бем М. В., Городиський І. М. Відповідальність за порушення законодавства про захист персональних даних: проблеми відповідності законодавства України вимогам регламенту Європейського Союзу щодо захисту персональних даних (GDPR). *Право України*. 2019. № 2. С. 237–255.
2. Бем. М. В., Городиський І. М. Стандарти захисту персональних даних в соціальній сфері. Львів: б.в., 2018. 110 с.
3. 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.
4. Бобрик В. І. Право власності на персональні дані. *Вісник Хмельницького інституту регіонального управління та права*. 2002. № 2. – С. 114–117.
5. Брижко В. М., Радянська А. І., Швець М. Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. К.: Тріумф, 2006. 256 с.
6. Булеца С. Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету. Сер.: : Право*. 2014. Вип. 25. С. 56–61.
7. Гронь О., Погореленко А. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство*. 2018. Вип. 19(1). С. 102–108.
8. Дмитренко, Олена Анатоліївна. Право фізичної особи на власні персональні дані в цивільному праві України : дис. ... канд. юрид. наук : 12.00.03 / НДІ приват. права і підприємництва Акад. прав. наук України. – К., 2010. – 210 с.
9. Жорж М., Саттон Г. Аналіз Закон України «Про захист персональних даних». Страсбург, 2012. 45 с.
10. 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.

11. Каретник О. С. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України. *Часопис Київського університету права*. 2013. № 2. С. 228–231.

12. Косіцин М., Плешко Е. Проблемні питання правового регулювання повноважень Держспецзв'язку України із захисту інформації про персональні дані *Прав., нормат. та метрол. забезп. системи захисту інформації в Україні*. 2010. Вип. 2. С. 10–13.

13. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України*. 2013. № 3. С. 123–126.

14. Макушев П. В. Персональні дані як елемент системи інформаційного забезпечення державної виконавчої служби України. *Форум права*. 2013. № 2. С. 333–339.

15. Макушев П. В. Системи інформаційного забезпечення державної виконавчої служби України та персональні дані як їх складові. *Право і суспільство*. 2013. № 4. С. 70–76.

16. Нагнічук О. І. Співвідношення права на свободу вираження щодо публічних осіб та права на повагу до приватного та сімейного життя публічних осіб у практиці Європейського суду з прав людини. *Наукові записки НаУКМА. Юридичні науки*. 2015. Т. 168. С. 72–77.

17. Олійник В. С. Конституційне право людини на особисту недоторканність і його забезпечення органами внутрішніх справ України: дис. … кандидата юрид. наук : 12.00.02 «Конституційне право» / Київськ. нац. ун-т внутр. справ. Київ, 2006. 225 с.

18. Оніщенко О. В. Персональні дані працівників: деякі особливості використання. *Вісник Академії адвокатури України*. 2012. Число 3. С. 173–175.

19. Пазюк А. В. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україна К. : МГО «Прайвесі Юкрейн», 2001. 260 с.

20. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : Автореф. дис... канд. юрид. наук : 12.00.11; Київ. нац. ун-т ім. Т. Шевченка. К., 2004. 19 с.

21. Погребна А. Коментар до Закону України «Про захист персональних даних» *Юридичний журнал*. 2010. № 7. URL – http://www.justinian.com.ua/article.php?id=3579 (дата звернення 30.04.2021).

22. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. 216 с.

23. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. 432 с.

24. Романюк І. Особливості змісту та реалізації права на персональні дані в Україні та зарубіжних країнах. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2013. Вип. 2. С. 102–106.

25. Романюк І. І. Персональні дані особи як об'єкт цивільного обороту. *Право і суспільство*. 2014. № 6.1(2). С. 58–65.

26. Сопілко І. М. Генезис змісту категорії «персональні дані». *Юридичний вісник. Повітряне і космічне право*. 2013. № 4. С. 62–66.

27. Сопілко І. М. Щодо вдосконалення системи захисту персональних даних в процесі їх обробки. *Форум права*. 2013. № 1. С. 939–945.

28. Чанишев р. І. Інформація про персональні дані працівника та її захист. *Актуальні проблеми держави і права*. 2010. Вип. 52. С. 94–99.

29. Чанишева Г. І., Чанишев р. І. Право на інформацію за трудовим законодавством України : монографія. О. : Фенікс, 2012. 193, [1] с.

30. Щербіна А. О., Макушев П.В. Персональні дані в системі інформаційного забезпечення органів місцевого самоврядування. *Публічне право*. 2013. № 3. С. 39–46.

Б. Іноземна спеціальна література

1. Bennett C. J. Regulating Privacy: Data Protection and Public Policy in Europe and the United State Itaca, NY : Cornell University Press, 1992.

2. Brouwer F. de. *Protection of Personal Data: a New Belgian Legal Framework Revue de Droit Des Affaires Internationales*. 1999. No. 2. Pp. 181–206.

3. Bukaty P. The California Consumer Privacy Act (CCPA) : an implementation guide. Ely, Cambridgeshire, United Kingdom : IT Governance Publishing, 2019.

4. Carey P. Data Protection: A Practical Guide to UK and EU Law : 3rd Edt. Oxford University Press, Inc. New York, NY, USA : 2009.

5. Dumortier J. The Protection of Personal Data in the Schengen Convention International Review of Law Computers and Technology, Cambridge. 1997. March. Vol. 11. No. 1. P. 93–106.

6. Finlyson D., Moore M. Data protection in legal practice : the Infolegal guide to GDPR and the Data Protection Act 2018. London : Infolegal, 2019.

7. Fleischmann A. Personal Data Security: Divergent Standards in the European Union and the United States. *Fordham International Law Journal*. 1995. October. Vol. 19. No. 1. Pp. 143–180.

8. Heisenberg D. Negotiating Privacy: The European Union, the United States, and Personal Data Protection Boulder, CO, USA: Lynne Rienner Publisers, 2005.

9. Krzysztofek M. GDPR : General Data Protection Regulation (EU) 2016/679 : post-reform personal data protection in the European Union. Alphen aan den Rijn, The Netherlands : Wolters Kluwer, 2019.

10. Kuner C., Bygrave L.A., Docksey C.A., Dreschler L. The EU General Data Protection Regulation (GDPR) : a commentary. Oxford : Oxford University Press, 2020.

11. Pearce G., Platten N. Achieving Personal Data Protection in the European Union. *Journal of Common Market Studies*. 1998. Vol. 36. No. 4. Pp. 529–547.

12. Platten N. Orchestrating Transatlantic Approaches to Personal Data Protection: a European Perspective. *Fordham International Law Journal*. 1999. June. Vol. 22. No. 5. Pp. 2024–2051.

13. Rosemary J. Guide to the General Data Protection Regulation a companion to Data protection law and practice : 4th edition. London Sweet & Maxwell, 2017.

14. Simitis S. Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data. *European Law Journal*. 1999. March. Vol. 5. No. 1. Pp. 45–62.

15. Ukrow J. Practitioner's Corner · Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108. *European data protection law review*. Vol. 4, No. 2. 2018. Pp. 239–247.

16. Warren S., Brandeis L. Rights to Privacy. *Harvard Law Review*. 1890. Vol. 4, No. 5. Pp. 193–220.

B. Міжнародні 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. URL: http://www.oecd.org/sti/iecon-omy/2013-oecd-privacy-guidelines.pdf (Date of request: 30.04.2021).

2. Principles relating to the Status of National Institutions (The Paris Principles) : Adopted by General Assembly resolution 48/134 of 20 December 1993. URL: https://www.ohchr.org/EN/ProfessionalInterest/Pages/StatusOfNationalInstitutions.aspx (Date of request: 16.05.2021).

3. Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data) of 18th May, 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (Date of request: 2021).

4. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. *Офіційний вісник України*. 2011. 14 січ. (№58). Ст. 701.

5. 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. *Офіційний вісник України*. 2011. 14 січ. (№58). Ст. 708.

6. 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 URL: http://zakon4.rada.gov.ua/laws/show/994_242 (Дата звернення: 30.04.2021)

7. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 23.05.2021 р.)

Г. Національне законодавство

1. 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. С. 42, стаття 1954, код акта 57277/2011.

2. Про доступ до публічної інформації : Закон України від 13 січня 2011 р. №2939-VI. Голос України. 2011. 09 лют. (№24).

3. Про затвердження документів у сфері захисту персональних даних : Наказ № 1/02-14 від 08.01.2014 р. Баланс. 2014, 06 бер. 2014. № 19. Ст. 5.

4. 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. С. 199, стаття 1604, код акта 51762/2010.

5. 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. С. 122, стаття 3771, код акта 64640/2012.

6. Про інформацію : Закон України 2657-XII від 02 жовтня 1992 р. *Відомості Верховної Ради України*. 1992. 01 груд. (№48). Ст. 650.

Ґ. Законодавство зарубіжних країн

1. Велика Британія: Data Protection Act 2018 URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (date requested: 30.04.2021).
2. Ірландія: Data Protection Act, URL: http://www.irishstatutebook.ie/1988/en/act/pub/0025/print.html (date requested: 30.04.2021).
3. Італія: Data Protection Code – Legislative Decree no. 196/2003 URL : http://www.privacy.it/privacycode-en.html (date requested: 30.04.2021).
4. Німеччина: Federal Data Protection Act in the version promulgated on 14 January URL: http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf (date requested: 30.04.2021).
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) URL: http://www.giodo.gov.pl/144/id_art/171/j/en/ (date requested: 30.04.2021).
6. Чехія: Act No. 101/2000 Coll., of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts. URL: https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1107 (date requested: 30.04.2021).
7. Чорногорія: Personal Data Protection Law URL: http://www.afapdp.org/wp-content/uploads/2012/01/Mont%C3%A9n%C3%A9gro-Personal-Data-Protection-Law-79-08-and-70-09.pdf (date requested: 30.04.2021).

Маркіян Бем, адвокат, канд. юрид. наук, старший юрист ЮФ «Василь Кісіль і Партнери». У 2013–2015 рр. працював на посаді Представника із захисту персональних даних Уповноваженого Верховної Ради України з прав людини. У 2015–2019 рр. – юрист Європейського суду з прав людини. Викладав у Школі права Українського католицького університету, в якості експерта співпрацює із Радою Європи та ОБСЄ. Автор низки публікацій із тематик міжнародного права, практики ЄСПЛ та захисту персональних даних.

Іван Городиський, адвокат, канд. юрид. наук, керуючий партнер ЮФ «Дексіс Партнерс». У 2014–2020 рр. директор-засновник Школи права Українського католицького університету. З 2021 р. директор Центру Дністрянського. В якості експерта співпрацює із Радою Європи та World Justice Project. Член Правління Асоціації правників України. Автор низки публікацій із тематик міжнародного права та захисту персональних даних.

UKR

Рада Європи є провідною організацією із захисту прав людини на континенті. Вона нараховує 47 держав-членів, включно з усіма державами – членами Європейського Союзу. Усі держави – члени Ради Європи приєдналися до Європейської конвенції з прав людини – договору, спрямованого на захист прав людини, демократії та верховенства права. Європейський суд з прав людини здійснює нагляд за виконанням Конвенції у державах-членах.

www.coe.int

Держави – учасниці Європейського Союзу вирішили поєднати свої ноу-хау, ресурси та долі. Разом вони збудували зону стабільності, демократії та сталого розвитку, зберігаючи при цьому культурне розмаїття, толерантність та громадянські свободи. Європейський Союз прагне поділитися своїми досягненнями та цінностями з країнами та народами за його межами.

www.europa.eu

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE