Принципи захисту персональних даних закріплені в законодавстві ЄС.

1. Поняття та зміст принципів захисту та обробки персональних даних.
2. Принципи законності, чесності та прозорості обробки персональних даних.
3. Принцип безпеки та ефективного захисту персональних даних. Принцип підзвітності персональних даних.
4. Принцип обмеження зберігання. Принцип цілісності та безпеки.
5. Принцип справедливої обробки персональних даних.
6. Принципи адекватності, відповідності та ненадмірності персональних даних.

Поняття та зміст принципів захисту та обробки персональних даних.

Принципи є відправними точками для більш детальних положень у наступних статтях регламенту. Вони також з'являються у статтях 5, 7, 8 та 10 Оновленої Конвенції 108. Подальше законодавство із захисту даних на рівні РЄ та ЄС має відповідати цим принципам, і їх необхідно враховувати при тлумаченні цього законодавства. Відповідно до права ЄС обмеження щодо цих принципів обробки дозволяються тільки в тій мірі, в якій вони відповідають правам та обов'язкам, передбаченим статтями 12–20, вони також повинні поважати суть основоположних прав та свобод.

В узагальненому вигляді вказані принципи можна викласти так: 1) законність і справедливість (англ. fairness, станом на сьогодні цей принцип частіше формулюється як принцип прозорості обробки персональних даних); 2) легітимної мети; 3) пропорційність до персональних даних до легітимної мети; 4) точність (вірогідність), актуальність персональних даних; f 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. 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 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 та ст. 5 Конвенції) – розширений виклад принципу законності і т. д.

Принципи законності, чесності та прозорості обробки персональних даних.

Принцип законності обробки.

Правові норми Європейського Союзу та Ради Європи, що регулюють захист персональних даних, встановлюють вимогу щодо законної обробки цих даних. Для визнання законності обробки персональних даних необхідна згода суб'єкта цих даних або наявність іншої законної підстави, передбаченої відповідним законодавством з питань захисту персональних даних270. Стаття 6 (1) Загального регламенту з питань захисту персональних даних (GDPR) надає п'ять правомірних підстав для обробки

даних, зокрема, якщо обробка є необхідною для виконання договору, виконання завдань в межах владних повноважень, виконання юридичного обов'язку, захисту легітимних інтересів контролера або третьої сторони, або в разі необхідності для захисту життєво важливих інтересів суб'єкта персональних даних.

Правовий акт повинен не лише надавати санкції для права на збір даних, але й визначати докладні правила їх обробки. Щодо цієї аспектуальної сторони, принцип законності був ретельно розглянутий в практиці Європейського суду з прав людини (ЄСПЛ). Відповідно до статті 8 Європейської конвенції про захист прав людини втручання в забезпечені нею права (зокрема, право на повагу до приватного життя, що включає право на захист персональних даних) можливе лише у випадках, коли це відбувається "згідно із законом".

Термін "згідно із законом" вимагає не лише наявності певної правової основи в "законі", але також встановлює вимогу до якості цього "закону", зазначаючи, що він повинен бути доступним для осіб, які стосуються цього, і передбачуваним щодо наслідків його застосування. Вимога доступності зазвичай виконується, якщо відповідний нормативно-правовий акт оприлюднений. Щодо вимоги передбачуваності, ЄСПЛ встановив, що норма є "передбачуваною", якщо вона сформульована чітко і достатньо, щоб особа могла, за необхідності, регулювати свою поведінку, користуючись відповідною допомогою (див. рішення у справі "Ротару проти Румунії", заява № 27798/95, п. 48–49).

Приклад 1.

У справі "Ротару проти Румунії" (Rotaru v. Romania), Служба розвідки Румунії (далі - СР) утримувала файл, що включав особисті дані заявника, такі як інформація про навчання, громадську активність, публікації, участь у політичних організаціях тощо. Заявник стверджував, що зберігання цієї інформації СР було незаконним. Суд визначив, що єдиною

підставою для такого накопичення була норма в законі про СР, яка дозволяла їй збирати, зберігати та використовувати інформацію, важливу для національної безпеки. Однак суд відзначив, що закон не визначав межі використання цих повноважень. Законодавство не передбачало, яка інформація може бути збережена, категорії осіб, щодо яких може збиратися інформація, обставин, при яких може відбуватися збір інформації, процедури збору, строків зберігання такої інформації, хто має доступ до файлів, як вони можуть використовуватися та який характер цих файлів. Суд також зауважив, що зберігання та використання цієї інформації не супроводжувалися відповідними гарантіями від зловживань, зокрема не було незалежного контролю (наприклад, судового) за діяльністю СР в цій частині. З урахуванням цих фактів суд визначив, що законодавство, яке регламентувало втручання в права заявника (обробка СР його персональних даних), не було достатньо передбачуваним. Таким чином, втручання в права заявника було незаконним і порушувало статтю 8 Конвенції.

Принцип чесності обробки.

У додаток до вимог щодо законності обробки, право ЄС та РЄ з захисту персональних даних встановлює вимогу, згідно з якою персональні дані повинні оброблятися чесно271. Принцип чесної обробки в основному регулює взаємовідносини між контролером та суб'єктом персональних даних. Контролери мають зобов'язання інформувати суб'єкта даних та громадськість про те, що обробка персональних даних відбуватиметься законно та прозоро, і повинні мати можливість продемонструвати відповідність операцій обробки положенням Загального регламенту з питань захисту персональних даних (ЗРЗПД). Операції з обробки даних не повинні бути приховані, і суб'єкт персональних даних повинен бути інформований про потенційні ризики. Крім того, контролер повинен діяти

таким чином, який надає можливість негайно враховувати бажання суб’єкта даних, особливо, якщо обробка ґрунтується на згоді суб’єкта.

Що стосується інтернет-послуг, характеристики систем обробки даних мають надавати суб’єкту персональних даних можливість дійсно розуміти, що відбувається з його персональними даними. У будь-якому разі принцип чесності обробки є ширшим, ніж обов’язок прозорості, та може бути пов’язаний з етичними аспектами обробки персональних даних.

Приклад 2.

Дослідницький департамент університету проводить експеримент з аналізу зміни настрою в 50 осіб. Згідно з правилами експерименту, вимагалося реєструвати їхні думки щогодини у електронних файлах у визначений час. Початково 50 осіб надали свою згоду на таке використання їхніх даних університетом. Проте пізніше департамент виявив, що ці дані можуть бути корисні іншому проєкту з розумового здоров'я, який координується іншою командою. Навіть при тому, що університет, як контролер, міг би використовувати ті самі дані для роботи іншої команди без додаткових заходів щодо законності обробки цих даних, оскільки ці цілі є сумісними, університет вирішив сповістити суб’єктів даних і запитати нової згоди відповідно до їхнього Кодексу етики досліджень та принципу чесності обробки.

Принцип прозорості обробки.

Згідно із законодавством ЄС та нормативно-правовими документами РЄ, обробка персональних даних повинна відбуватися "у прозорий спосіб щодо суб’єкта персональних даних". Цей принцип вимагає від контролера персональних даних вживати належні заходи для інформування суб’єктів персональних даних – таких як користувачі, покупці чи клієнти – про те, як використовуються їхні особисті дані. Прозорість може охоплювати інформацію, яка надається суб’єктам даних перед початком обробки,

інформацію, яка повинна бути готовою та доступною суб’єкту даних під час обробки, а також відповідь на запити суб’єктів щодо доступу до їхніх даних.

Суб’єкти персональних даних мають бути повідомлені про операції з обробки способом, що легко сприймається та доступний, гарантуючи їм зрозуміння процесу використання їхніх особистих даних. Це передбачає, що суб’єкт даних повинен мати інформацію про конкретну мету обробки персональних даних ще на етапі їх збирання. Принцип прозорості обробки передбачає використання зрозумілого та простого мовлення, забезпечуючи зрозумілість щодо ризиків, правил, гарантій та прав щодо обробки їхніх персональних даних.

Право РЄ встановлює обов'язок контролера передбачати важливу інформацію та надавати її суб'єкту даних активно. Ця інформація повинна включати назву та адресу контролера (або спільних контролерів), юридичну підставу, цілі обробки даних, категорії оброблюваних даних, одержувачів та засоби реалізації прав. Контролер може надавати цю інформацію у різних форматах, таких як вебсайт, технологічні сервіси на особистий пристрій тощо, забезпечуючи її чесність та ефективність. Інформація повинна бути доступною, читабельною, зрозумілою та адаптованою для конкретного суб'єкта даних, включаючи використання зручної для дитини мови, якщо це необхідно.

Крім того, контролер повинен надавати будь-яку додаткову інформацію, яка сприяє чесності обробки персональних даних або є корисною для цієї мети, таку як період зберігання даних, обґрунтування підстав обробки даних або інформація про передачу даних одержувачам в інші держави-учасниці. Суб'єкт даних має право отримувати інформацію від контролера щодо того, чи обробляються його дані і, у випадку позитивної відповіді, які саме дані обробляються. Перед початком обробки контролери або оператори повинні повідомляти осіб, чиї дані

обробляються, про цілі, тривалість, засоби обробки та інші деталі відповідно до права на інформацію.

Приклад 3.

У справі "Смаранда Бара та інші проти Національного фонду медичного страхування та інших", розглядається передача податкових даних, що стосуються доходів самозайнятих осіб, з Національного агентства податкового адміністрування до Національної агенції страхування здоров'я в Румунії. З цих даних були винесені вимоги щодо сплати боргів за страхування здоров'я. Питання, яке постало перед Судом Європейського Союзу (СЄС), стосувалося того, чи були суб'єкти персональних даних повинні бути повідомлені про ідентифікаційні дані контролера та цілі передачі даних до того, як агентство податкового адміністрування почало їх обробку. СЄС вирішив, що в ситуації, коли один орган держави-члена передає персональні дані іншому органу, який подальше їх обробляє, суб'єктам даних повинно бути повідомлено про передачу та обробку цих даних.

Принцип безпеки та ефективного захисту персональних даних. Принцип підзвітності 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 даних75. 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 безпеки76. 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.

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 порушення73. 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».

Принцип обмеження зберігання. Принцип цілісності та безпеки.

У статті 5 (1) (e) ЗРЗПД, а також у статті 5 (4)(e) Оновленої Конвенції 108 від держав-членів вимагається забезпечити збереження персональних даних «у формі, що дозволяє встановлювати особу суб'єктів персональних даних не довше, ніж це необхідно для цілей», для яких вони обробляються. Тому персональні дані повинні бути видалені або знеособлені, якщо мета була досягнута. Для цього «мають бути встановлені строки для видалення або періодичного перегляду», щоб дані не зберігалися довше, ніж це необхідно.

У справі «С. та Марпер» ЄСПЛ дійшов висновку, що основні принципи відповідних документів Ради Європи, законодавство і практика інших Договірних Сторін вимагають, щоб збереження даних було пропорційним меті збирання та обмежувалось у часі, особливо стосовно діяльності поліції.

Приклад 8.

У справі «С. та Марпер» ЄСПЛ вирішив, що зберігання протягом невизначеного періоду відбитків пальців, зразків клітин та ДНКпрофілів

двох заявників було непропорційним та не необхідним у демократичному суспільстві, враховуючи, що кримінальне провадження проти обох заявників закінчилося їхнім виправданням та закриттям справи.

Обмеження часу зберігання персональних даних застосовується тільки до тих даних, які зберігаються у формі, що дозволяє ідентифікацію суб'єкта даних. Відповідно, законність зберігання даних, які вже не є необхідними, може бути забезпечена шляхом знеособлення даних. Персональні дані, збережені з метою історичного, статистичного чи наукового використання, можуть зберігатися довший час за умови, що такі дані будуть використовуватись виключно для зазначених цілей. Для подальшого збереження та використання персональних даних мають бути запровадженні належні технічні та організаційні заходи для гарантування прав та свобод суб'єкта персональних даних. Оновлена Конвенція 108 також дозволяє винятки з принципу обмеженого зберігання даних за умови, що вони передбачені законом, поважають суть основоположних прав та свобод та є необхідними і пропорційними для досягнення обмеженої кількості легітимних цілей. Вони, серед іншого, включають захист національної безпеки, розслідування злочинів та переслідування за їх вчинення, виконання кримінальних покарань, захист суб'єкта даних та захист прав і свобод інших.

Приклад 9.

У справі "Digital Rights Ireland" Суд ЄС перевіряв законність Директиви про зберігання даних, яка мала на меті уніфікацію національних положень щодо зберігання персональних даних, що виникають або обробляються в результаті функціонування публічно доступних електронних комунікаційних послуг чи суспільних телекомунікаційних мереж для можливого передавання компетентним органам у боротьбі з серйозними злочинами, такими як організована злочинність чи тероризм.

Директива про зберігання даних передбачала, що дані можуть зберігатися протягом "принаймні шести місяців без будь-якого розрізнення між категоріями даних, передбачених статтею 5 Директиви, на підставі їхньої можливої корисності для переслідуваних цілей або відповідно до осіб, яких це стосується". Суд ЄС також висунув питання про відсутність об'єктивних критеріїв в Директиві, на основі яких конкретний термін зберігання - який може варіюватися від шести до максимальних 24 місяців - мав бути визначений для забезпечення обмеження цього періоду до абсолютно необхідного рівня.

Принцип безпеки даних вимагає вживання організаційних або технічних заходів під час обробки персональних даних для їх захисту від випадкового, несанкціонованого або протиправного доступу, використання, зміни, відкриття, втрати, знищення або пошкодження. Закон про захист персональних даних визначає, що при впровадженні заходів безпеки контролер та оператор повинні враховувати "сучасний стан справ, витрати на впровадження та характер, обсяг, контекст і мету обробки, а також ризики різного ступеня вірогідності та серйозності для прав та свобод фізичних осіб."

В залежності від обставин конкретного випадку відповідні технічні та організаційні заходи можуть включати псевдонімізацію та шифрування даних, а також регулярну перевірку та оцінку ефективності цих заходів для забезпечення безпеки обробки даних. Псевдонімізація даних означає заміну елементів персональних даних, які ідентифікують суб’єкта даних, на псевдоніми та зберігання цих елементів окремо за допомогою технічних та організаційних заходів. Важливо відзначити, що псевдонімізацію не слід плутати зі знеособленням, де всі зв'язки, що ідентифікують особу, розриваються. Псевдонімізовані дані використовуються як засіб для збереження конфіденційності осіб у різних контекстах, наприклад, при дослідженні хвороби пацієнтів, де ідентифікація відома лише лікарні.

Таким чином, псевдонімізація відіграє ключову роль у забезпеченні конфіденційності та може бути важливим компонентом в системі обробки персональних даних, що враховує їх захист з самого початку.

У випадках витоку персональних даних як Оновлена Конвенція 108, так й ЗРЗПД вимагає від контролера без затримки повідомити компетентний наглядовий орган про витік даних та ризики для прав і свобод фізичних осі. Такий же обов'язок повідомлення суб'єкта даних існує у випадках, коли витік персональних даних може призвести до значних загроз для його прав і свобод. Повідомлення суб'єктів даних про такі витоки мають бути здійснені простою та ясною мовою. Якщо оператору стало відомо про порушення захисту персональних даних, контролер має бути повідомлений про це негайно. За певних обставин можуть застосовуватися винятки з зобов'язання здійснювати повідомлення. Наприклад, контролер не має повідомляти компетентний наглядовий орган у випадку, коли «малоймовірним є ризик для прав і свобод фізичних осіб внаслідок витоку даних». Також не потрібно повідомляти суб'єкта даних у разі, якщо застосовані заходи безпеки роблять дані незрозумілими для осіб, які не уповноважені мати до них доступ, або якщо в результаті подальших заходів здійснення загрози стає малоймовірною. Якщо повідомлення суб'єктів даних про порушення захисту даних покладає на контролера непропорційний тягар, публічне повідомлення або схожий захід може забезпечити «повідомлення суб'єктів даних таким саме ефективним шляхом».

Принцип справедливої обробки персональних даних.

Вказаний принцип закріплено як у Конвенції №108+ (п. (а) 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». 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.

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). 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.

Принципи адекватності, відповідності та ненадмірності персональних даних.

Згідно з вказаним принципом, склад та зміст персональних даних, що обробляються володільцем, повинні відповідати легітимній меті їх обробки та бути відповідними, адекватними та ненадмірними щодо такої мети. Це передбачає, що: Обробка повинна обмежуватися лише тими даними, які є необхідними для досягнення конкретної мети.

Якщо можливо досягти мети без обробки певних даних, така обробка не відповідає закону, навіть якщо вказані дані можуть бути використані для досягнення цілі.

Приклад 6.

У справі "L. H. v. LATVIA" (68, 1997 рік), заявниці довелося терміново робити кесарів розтин, але хірург, без її згоди, провів стерилізацію. Після цього інциденту інспекція, що контролювала якість надання медичної допомоги, зібрала відомості про медичну допомогу, надану заявниці з 1996 по 2003 роки. Заявниця оскаржила збір чутливої інформації про неї інспекцією, але суди відмовили у задоволенні її позову. При розгляді питання про необхідність збору інформації щодо заявниці, Суд зазначив, що інспекція зібрала надто великий обсяг інформації (за семирічний період) для оцінки лише одного хірургічного втручання в 1997 році. Такий обсяг

інформації не був обґрунтований. Суд визнав це втручання в права заявниці непропорційним і порушуючим статтю 8 Конвенції.

Обробка повинна виконуватися за допомогою засобів та методів, які відповідають визначеним цілям обробки, згідно з пунктом 2 частини 1 статті 6 Закону.

Приклад 7.

Міністерство охорони здоров'я (МОЗ) через Департамент охорони здоров'я обласної державної адміністрації (далі – Департамент) подало запит до лікарні щодо передачі копій обмінних карт вагітних із результатами допологових обстежень у випадках народження дітей із синдромом Дауна. Лікарня відповіла на запит, і відповідно до нього були направлені вказані документи. Згідно із запитом, ці документи потрібні для проведення дослідження, яке має на меті удосконалення пренатальної діагностики медичними закладами. Подальше направлення цих документів було адресовано вказаному дослідникові. Оскільки вказане наукове дослідження планувалося проводити саме дослідник, передача копій документів, що містять конфіденційну інформацію про стан здоров'я, Департаментові / МОЗ, а не дослідникові, не була обов'язковою. Крім того, для проведення цього дослідження не потрібно було використання особистих даних пацієнтів (імені, прізвища та по батькові). Для дослідження вистачало лише медичної інформації. Лікарня отримала відносно невелику кількість копій обмінних карт, і знеособлення цих документів не становило б значущого тягаря для медичного закладу. Проте такі дії лікарні також порушували вказані положення Закону.

Принцип пропорційності вимагає, щоб не лише самі дані були відповідними, а й спосіб їх обробки також відповідав критерію пропорційності. Обробка персональних даних повинна тривати лише стільки, скільки це необхідно для законних цілей, для яких вони збирались або оброблялися. Також рівень захисту персональних даних повинен бути

пропорційним характеру та обсягу даних, що обробляються. Це включає в себе визначення адекватних організаційно-технічних заходів захисту відповідно до обсягу та характеру персональних даних. Хоча це не є прямою вимогою Закону, міжнародні документи вказують на те, що заходи захисту персональних даних повинні бути "відповідними" згідно зі статтею 32 Регламенту та статтею 7 Конвенції.

Вказаний принцип має визначати будь-який процес обробки персональних даних, незалежно від підстав проведення цієї обробки. Навіть у випадку, коли особа надає згоду на обробку своїх персональних даних, які за своєю суттю не є необхідними для досягнення мети обробки, така обробка буде порушенням законодавства. Тому ситуації, де особа надає "необмежену згоду на обробку персональних даних" або "безвідкличну згоду", є неприйнятними. Чітко визначена мета повинна надавати власникові можливість з високим ступенем ймовірності передбачити обсяг персональних даних, необхідних для досягнення цієї мети.

Якщо обробка персональних даних здійснюється для виконання повноважень державного органу, оброблятися повинні лише ті дані, які є необхідними для належного виконання цих повноважень. Оскільки обробка в таких випадках здійснюється на підставі закону та в порядку, визначеному законодавством, нормативно-правові акти повинні визначати склад даних, який є пропорційним меті їх обробки, та спосіб відповідної обробки.

Тому пропорційність обробки повинна бути закладена в нормативно-правовий акт ще на етапі проекту. Обґрунтування того, чому проєкт нормативно-правового акта передбачає певний обсяг персональних даних для обробки, термін, метод обробки тощо, повинно бути відображено в пояснювальній документації до законопроєкту. Оскільки не завжди можна передбачити оптимальний обсяг даних, необхідних для виконання повноважень державного органу, законодавство повинно надавати державному органові певну дискрецію для врахування індивідуальної

ситуації суб'єкта персональних даних. Наприклад, у випадку звернення суб'єкта щодо припинення обробки, зміни чи виправлення його персональних даних, державний орган повинен мати можливість вжити відповідних заходів. Це відповідає вимогам статті 8 Закону, яка передбачає, серед іншого, право заперечення проти обробки, а також право вимагати виправлення власних персональних даних.

Література.

«Rotaru v. Romania», заява № 28341/95.
Оновлена Конвенція 108, стаття 5 (3);

Загальний регламент захисту персональних даних, стаття 5 (1) (a).

Хартія основних прав ЄС, стаття 8 (2);

Загальний регламент захисту персональних даних, п. 40 та статті 6–9;

Оновлена Конвенція 108, стаття 5 (2);

Пояснювальна записка до Оновленої Конвенції 108, п. 41.

Загальний регламент захисту персональних даних, стаття 5 (1) (a);

Оновлена Конвенція 108, стаття 5 (4) (a).

Рішення ЄСПЛ у справі «К. Г. та інші проти Словаччини» (K.H. and Others v. Slovakia), № 32881/04, від 28 квітня 2009 р.

Рішення Суду ЄС, C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших» (Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others), від 1 жовтня 2015р, пп. 28–46.

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: 01.01.2024).

Суд ЄС, об’єднані справи C-293/12 та C-594/12, «“Digital Rights Ireland Ltd.” проти Міністра зв’язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші»

(Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [ВП]), від 08 квітня 2014 р.

М. Бем, І. Городський. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. – «К.І.С.»., 2021. С. 161.