

Зміст ключових термінів у сфері захисту персональних даних.

1. Сутність, зміст та види персональних даних.
2. Обробка та знеособлення персональних даних
3. Поняття «володілець та розпорядник персональних даних»
4. Головні аспекти концепції персональних даних

Сутність, зміст та види персональних даних.

Поняття "персональні дані" визначається як інформація, яка стосується ідентифікованої особи або особи, яку можна ідентифікувати. У регулюючих документах, таких як Регламент, Директива, Конвенція та Закон, визначення цього поняття майже однакове. Основна ідея полягає в тому, що персональні дані - це інформація, пов'язана з конкретною особою.

Очевидно, що розуміння терміну "персональні дані" зумовлене основною їх властивістю - ідентифікацією (встановленням) фізичної особи. Згідно з європейським розумінням, поняття "персональні дані" слід трактувати наступним чином:

1. Дані набувають характеру персональних, якщо вони містять інформацію про вже відому (встановлену, визначену, ідентифіковану) особу або особу, яку можна встановити;

2. Особа, яку можна встановити, тає таку, яку можна ідентифікувати як за допомогою вже наявних даних, так і за допомогою додаткової інформації, отримання якої не потребує істотних зусиль;

3. Встановлення особи розглядається як процес, який може бути здійснений будь-яким суб'єктом, якому стали відомі або будуть відомі персональні дані в ході їх запланованого оброблення (іншими словами, якщо процес оброблення інформації передбачає ідентифікацію особи, то будь-який суб'єкт, що бере в ньому участь, зобов'язаний виконувати правові вимоги щодо захисту персональних даних);

4. Процес встановлення особи повинен складатися з елементів, що описують людину так, що дає можливість безпомилково виділити її серед

усіх інших людей (найяскравішим елементом такого опису є ім'я фізичної особи, або схожий ефект може забезпечити знання про те, що особа займає високу публічну посаду, наприклад Міністра);

5. Дані, які не мають жодних ідентифікаторів (анонімні, знеособлені дані), які унеможливають встановлення особи, не вважаються персональними.

Термін "ідентифікована особа" вказує на особу, яку можна однозначно визначити на основі наявної в інформації, що перебуває під контролем володільця даних. Для визнання особи ідентифікованою зазвичай необхідні такі дані, як ім'я, прізвище, по батькові та реквізити документа, який посвідчує особу (наприклад, ідентифікаційний номер фізичної особи). Проте за певних умов вже наявна менша кількість інформації або певний обсяг іншої інформації може бути достатнім для того, щоб особу визнавали "якою, що може бути ідентифікованою".

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 уможливають 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 річизі 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 спеціальних категорій персональних даних повинна відбуватися лише в виняткових випадках і вимагає вищих стандартів захисту та поваги прав суб'єктів персональних даних. Такий підхід ґрунтується на тому, що вказані категорії даних містять інформацію, яка часто може бути використана для дискримінації відносно конкретного суб'єкта персональних даних. Подумати про наслідки можна, уявивши, якщо, наприклад, роботодавець без належної потреби вимагатиме від потенційних кандидатів на посаду вказувати в анкеті чи резюме відомості щодо їхнього расового чи етнічного походження або релігійних переконань для цілей працевлаштування. Таким чином, виділення спеціальних

категорій персональних даних призначене забезпечити, що їх обробка здійснюється лише в разі виняткової необхідності.

Приклад 1

У справі "Volker und Markus Schecke GbR та Хартмут Ейферт проти землі Гессен" щодо оприлюднення персональних даних отримувачів сільськогосподарських субсидій СЕС встановив, що юридичні особи можуть вимагати захисту згідно зі статтями 7 та 8 Хартії ЄС тільки в тій мірі, в якій офіційна назва юридичної особи ідентифікує одну або більше фізичних осіб. Право на повагу до приватного життя, у контексті обробки персональних даних за статтями 7 та 8 Хартії, стосується будь-якої інформації про ідентифіковану фізичну особу або особу, яку може бути ідентифіковано.

Суд ЄС визнав, що втручання в основоположні права на приватність та захист персональних даних отримувачів субсидій є непропорційним, коли порівнювати інтерес ЄС в забезпеченні прозорості надання субсидій та права осіб на захист особистих даних. Суд вирішив, що мета прозорості могла б бути досягнута заходами з менш серйозними наслідками для прав осіб. Однак у випадку оприлюднення інформації щодо юридичних осіб, отримавших субсидії, СЕС вважав, що це не порушує принцип пропорційності, оскільки серйозність порушення права на захист персональних даних різниться для юридичних та фізичних осіб.

Суд дійшов висновку, що вимагати від національних органів досліджувати, чи ідентифікує дані кожну юридичну особу, яка отримала субсидію, будь-яку пов'язану фізичну особу, було б необґрунтованим адміністративним тягарем. Таким чином, законодавство, яке передбачає загальне оприлюднення даних юридичних осіб, встановило справедливий баланс між конкурентними інтересами.

Обробка та знеособлення персональних даних

Відповідно до Закону, обробка персональних даних включає в себе "будь-яку дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптація, зміна, оновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем". Важливо відзначити, що обробка не обмежується виконанням цих дій з систематизованою сукупністю персональних даних багатьох осіб, але також охоплює будь-яке зберігання інформації про фізичну особу, навіть якщо ця інформація недоступна.

Наприклад, наявність будь-якого документа, що містить персональні дані особи, на робочому столі чи в сейфі державного службовця також вважатиметься обробкою персональних даних цієї особи. Термін "використання" персональних даних, який зустрічається в Законі, визначається як будь-які дії володільця щодо обробки цих даних, а також дії щодо їх захисту та передачі права обробки іншим суб'єктам відносин, пов'язаних із персональними даними, за згодою суб'єкта персональних даних чи відповідно до закону.

Отже, поняття "використання" та "захист" персональних даних пов'язані з терміном "обробка", що зазначається в Законі, і застосовуються в контексті збирання, зберігання, передачі та інших дій із персональними даними.

Справедливо відзначено, що відповідно до усталеної практики Ради Європи та Європейського Союзу, захист персональних даних не є елементом обробки, оскільки він не передбачає вчинення конкретних дій з самими персональними даними. Використання зазвичай розглядається як елемент обробки, але у деяких юрисдикціях (наприклад, у Німеччині)

використання може бути розглянуте окремо відносно обробки, розглядаючи його як окрему дію щодо персональних даних.

Приклад 2.

У справі "Барбулеску проти Румунії" заявник був звільнений за використання інтернету роботодавця протягом робочих годин, порушуючи внутрішні правила компанії. Роботодавець моніторив його спілкування, включаючи повідомлення приватного характеру, і ці дані були використані національним судом під час розгляду справи.

Європейський Суд з прав людини визнав застосовність статей 7 та 8 Європейської конвенції з прав людини (ЄКПЛ). Вирішуючи питання про те, чи були обмеження, встановлені роботодавцем, обґрунтованими щодо очікувань приватності, Суд визнав, що інструкції роботодавця не можуть анулювати право на приватне соціальне життя працівника, коли він перебуває на робочому місці.

Щодо необхідності встановлення законодавчого регулювання умов моніторингу спілкування працівників, Суд визначив, що держави-учасниці повинні користуватися широкими межами розсуду, але одночасно вони повинні забезпечити адекватні гарантії проти можливого зловживання. Пропорційність та процедурні гарантії проти свавілля визначались як суттєві, і Суд врахував обсяг моніторингу, ступінь втручання у приватне життя працівника, наслідки для працівника, та наявність належних гарантій.

У висновку Суд зазначив, що працівник, чия комунікація підлягала моніторингу, повинен мати можливість захисту в суді, який визначав би правомірність заходів та дотримання необхідних гарантій. У даній справі Європейський Суд з прав людини визнав порушення статті 8 ЄКПЛ, оскільки національні органи не забезпечили належного захисту прав

заявника на повагу до приватного життя та кореспонденції і не забезпечили справедливого балансу між конфліктними інтересами.

Отже, захист персональних даних розглядається як самостійна дія, відокремлена від їхньої обробки та використання. У цьому контексті важливо визначати та дотримуватися стандартів та правил, які забезпечують безпеку та конфіденційність персональних даних без прямого втручання в їхню обробку або використання. Розрізнення цих термінів і дій важливе для точного розуміння та застосування нормативів щодо захисту персональних даних в юридичному та практичному контексті.

Важливо відзначити, що Закон про захист персональних даних обмежується певними видами обробки персональних даних. Зокрема, він поширюється на такі види обробки:

1. Обробка із застосуванням автоматизованих засобів: Закон застосовується до будь-якої обробки, яка ведеться повністю або частково із застосуванням автоматизованих засобів, що включає в себе, наприклад, обробку даних за допомогою комп'ютерів.

2. Обробка персональних даних у картотеці: Закон охоплює обробку персональних даних у картотеці чи призначених для внесення до картотеки, із застосуванням неавтоматизованих засобів. Це включає в себе ручну обробку даних.

3. Обробка персональних даних, які поки не внесені в картотеку, але призначені для цього: Закон застосовується до обробки таких даних, навіть якщо вони на даний момент не внесені в картотеку, але призначені для цього.

Важливо враховувати, що неавтоматизована обробка персональних даних поза межами картотеки не підпадає під дію Закону. Крім того, Закон передбачає винятки для обробки персональних даних для приватних, журналістських і творчих цілей. Такі обробки можуть мати свої власні внутрішні механізми захисту даних відповідно до інших правил і обмежень.

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.

Так, вказане регулювання свідчить про те, що Закон про захист персональних даних має свої винятки для обробки даних у журналістських та творчих цілях. Закон не поширює свої положення на такі випадки, якщо забезпечено баланс між правом на повагу до особистого життя та правом на свободу вираження поглядів.

Приклад 3.

У справі "Боділ Ліндквіст" Європейський Суд вирішив, що дії, пов'язані із посиланнями на веб-сторінках на різних осіб та їхню ідентифікацію за допомогою імен або інших засобів, таких як телефонні номери чи інформація про хобі, вважаються "обробкою персональних даних повністю або частково автоматизованими засобами" в розумінні статті 3 (1) Директиви 95/46.

Це рішення вказує, що ідентифікація осіб за допомогою їхніх особистих даних, навіть якщо це відбувається через посилання на інтернет-сторінках, вважається процесом обробки персональних даних. Директива 95/46 визначає широкий спектр операцій, які можуть бути включені до поняття "обробка персональних даних", і це рішення визнає, що такі дії підпадають під це поняття.

Важливо враховувати, що у сфері журналістської діяльності можуть застосовуватися інші етичні та професійні стандарти, а також закони,

специфічні для журналістики, щоб забезпечити високий рівень дотримання принципів свободи слова та інших цінностей, характерних для журналістської професії.

У випадках, коли втручання в право особи на повагу до приватного життя через обробку її персональних даних може вважатися надмірним, порівняно з суспільним інтересом до висвітленої інформації, можуть виникнути питання щодо додержання законодавства про захист персональних даних. Такі випадки можуть піддаватися увазі регуляторів або судового розгляду для з'ясування справедливого балансу між свободою вираження і правом на захист особистих даних.

"Знеособлення" персональних даних визначається як вилучення інформації, яка може призвести до прямої чи опосередкованої ідентифікації особи. Цей процес є корисним для статистичних чи наукових досліджень, де потрібно обробити значні обсяги часто чутливих даних, не створюючи ризику втручання в права суб'єктів персональних даних.

Важливо розрізняти "знеособлення" персональних даних від терміну "псевдознеособлення" або "псевдонімізації", який використовується в Регламенті. "Псевдонімізація" за зазначеним Регламентом означає обробку персональних даних таким чином, що їх більше не можна віднести до конкретного суб'єкта даних без використання додаткової інформації. При цьому додаткова інформація повинна бути збережена окремо, і до неї повинні застосовуватися технічні та організаційні заходи для забезпечення того, що персональні дані стають невіднесеними до фізичної особи, яку ідентифіковано чи можна ідентифікувати.

Отже, при псевдонімізації володільцю даних залишається можливість в необхідний момент визначити, яку інформацію стосовно ідентифікованої (або особи, яку можна ідентифікувати) фізичної особи представляють відомості. У випадку знеособлення такої можливості для володільця даних вже не існує. Загалом, псевдонімізація є ефективним заходом захисту

персональних даних на організаційному рівні, спрямованим на зменшення кількості осіб, які мають доступ до персональних даних, що обробляються. Таким чином, введення визначення псевдонімізації в текст Закону здійснить стимул для його більш широкого використання.

Приклад 4.

У справі "Google Spain SL, Google Inc. проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса", Маріо Костеха Гонсалес вимагав прибрати або змінити зв'язок між його ім'ям у пошуковій системі Google та газетними сторінками, де оголошувався аукціон нерухомості для стягнення боргів у системі соціального страхування.

Європейський Суд визначив, що дії постачальника пошукових систем, таких як Google, у відношенні збору, витягування, запису, організації, зберігання і доступу до інформації, яка опублікована в Інтернеті, становлять "обробку" персональних даних. Незалежно від того, чи обробляється інформація про фізичних осіб чи інші дані, такі дії вважаються обробкою персональних даних згідно з визначенням Суду.

Отже, Суд прийняв рішення, що постачальник пошукових систем має обов'язок дотримуватися правил щодо захисту персональних даних при обробці інформації у своїх пошукових результатах, незалежно від характеру цієї інформації.

Поняття «володілець та розпорядник персональних даних»

Відповідно до визначення, наведеного в Законі, володільцем персональних даних є фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не передбачено законом (ст. 2). Таким чином, володільцем може бути:

Особа, яка самостійно визначає мету обробки, склад даних і процедури обробки.

Суб'єкт, визначений законом для конкретних випадків.

Це визначення відповідає положенням ключових міжнародних документів. Згідно з Конвенцією №108+, володільцем (або "контролером файлу", як перекладено на веб-сайті ВРУ) може бути фізична або юридична особа, державний орган, установа чи будь-яка інша установа, яка уповноважена відповідно до національного законодавства вирішувати, якою повинна бути мета файлу даних для автоматизованої обробки.

Регламент також надає адаптоване до сучасних умов визначення. Згідно зі ст. 4 Регламенту, "володільцем" є фізична чи юридична особа, орган публічної влади, агентство чи інша установа, яка самостійно чи спільно з іншими визначає мету та спосіб обробки персональних даних.

Таким чином, володільць персональних даних може бути особою чи організацією, яка самостійно визначає цілі та методи обробки даних або обрана відповідно до законодавства для конкретних випадків.

Відповідно до статті 2 Закону, розпорядник персональних даних – це «фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця».

Порівняно із Конвенцією № 108+, яка не використовує термін "розпорядник", відзначається тим, що відсутнє самостійне визначення цього терміну. Однак в директиві та регламенті використовується термін "розпорядник" зі схожим визначенням. У Регламенті та Директиві розпорядник – це «фізична чи юридична особа, орган публічної влади, агентство чи інша установа, яка обробляє персональні дані від імені володільця».

Відзначається, що визначення терміну "розпорядник" у Законі є практично ідентичним тому, яке використовується в Директиві та Регламенті. Отже, ймовірно, що термін і визначення були позичені з цих міжнародних документів.

Стаття 28 Регламенту розглядає особливості співпраці між володільцем та розпорядником персональних даних, надаючи низку гарантій для ефективного захисту прав суб'єктів персональних даних.

Відповідно до цієї статті, володільцю персональних даних покладено обов'язок обирати тільки тих розпорядників, які можуть забезпечити обробку даних відповідно до вимог Регламенту. При цьому розпорядник може призначати суброзпорядників лише за згодою володільця. Зв'язки між володільцем та розпорядником регулюються письмовим або електронним договором чи законом, які повинні визначати різноманітні аспекти обробки, такі як природа та мета обробки, тривалість, склад даних, категорії суб'єктів персональних даних, а також права та обов'язки володільця.

У випадку, якщо розпорядник доручає обробку отриманих від володільця даних іншому розпорядникові (суброзпорядникові), умови такого доручення повинні відповідати умовам, визначеним в договорі між володільцем та розпорядником. Важливо відзначити, що в разі порушення суброзпорядником обов'язків з захисту персональних даних, відповідальність за це несе сам розпорядник перед володільцем. Додатково, якщо розпорядник змінює мету або порядок обробки даних, він визнається володільцем в цій частині операцій з обробки, і відповідає за них в повному обсязі.

Головні аспекти концепції персональних даних

Відповідно до права ЄС вигодонабувачами правил захисту персональних даних можуть бути тільки фізичні особи, і тільки живі фізичні особи перебувають під захистом права із захисту персональних даних ЄС. Загальний регламент захисту персональних даних (ЗГЗПД) визначає персональні дані як будь-яку інформацію про ідентифіковану фізичну особу або фізичну особу, яку можна ідентифікувати.

Право РЄ, а саме Оновлена Конвенція 108 також вказує на захист фізичних осіб стосовно обробки їхніх персональних даних. У ній так само персональні дані означають інформацію стосовно ідентифікованої фізичної особи або фізичної особи, яку можливо ідентифікувати. Ця фізична особа або індивід, як визначає ЗГЗПД та Оновлена Конвенція 108, називається в праві із захисту персональних даних суб'єктом персональних даних.

Юридичні особи також користуються певним захистом у контексті обробки їхніх персональних даних. Європейський Суд з прав людини (ЄСПЛ) виносить рішення у справах, поданих юридичними особами, які стверджують, що порушено їхнє право на захист від використання їхніх даних відповідно до статті 8 Європейської конвенції з прав людини (ЄКПЛ). Ця стаття захищає право на повагу до приватного і сімейного життя, а також право на повагу до житла і кореспонденції.

Оновлена Конвенція 108 про захист персональних даних в першу чергу застосовується до захисту фізичних осіб. Проте держави-члени мають можливість розширити захист даних і на юридичних осіб, таких як компанії та об'єднання, через своє законодавство. Національний закон може розширити Конвенцію на юридичні особи з метою захисту їхніх інтересів.

Зазначено, що право Європейського Союзу з захисту персональних даних не поширюється на обробку даних, які стосуються юридичних осіб, зокрема підприємств, включаючи їх назву, форму та контактні дані. Однак Директива про конфіденційність та електронні комунікації забезпечує захист конфіденційності комунікації та легітимних інтересів юридичних осіб щодо автоматичного збереження та обробки даних, пов'язаних із підписниками та користувачами. Проєкт нової Директиви про конфіденційність та електронні комунікації також передбачає розширення захисту на юридичних осіб.

Концепція обробки персональних даних, як визначено як у праві Європейського Союзу, так і в праві Ради Європи, є складною та

інтегральною. Термін «обробка персональних даних» охоплює різноманітні операції, що здійснюються з особистою інформацією. Серед цих операцій входять збір, реєстрація, організація, структурування, зберігання, адаптація, зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження, надання іншим чином, упорядкування, комбінування, обмеження, видалення чи знищення. Оновлена Конвенція 108 доповнює визначення, включаючи аспекти збереження персональних даних.

У справі "Франтішек Ринеш" [193] господар Ринеш, використовуючи систему домашнього відеоспостереження, зафіксував зображення двох осіб, які вчинили акт вандалізму, розбивши вікна в його будинку. Європейський Суд з прав людини вирішив, що відеоспостереження, включаючи запис та збереження персональних даних, вважається автоматичною обробкою даних, яка підпадає під законодавство ЄС щодо захисту особистих даних.

Приклад 1

У справі "Франтішек Ринеш" господар Ринеш, використовуючи домашню систему телевізійного спостереження, зафіксував зображення двох осіб, що вчинили акт вандалізму, розбивши вікна його будинку. Суд Європейського Союзу вирішив, що відеоспостереження, включаючи запис та збереження персональних даних, вважається автоматичною обробкою даних, що підпадає під законодавство ЄС з захисту персональних даних. Це рішення визначило, що така форма відеонагляду належить до категорії обробки даних, і повинна підпадати під відповідні норми та стандарти щодо захисту приватності осіб, визначені законодавством Європейського Союзу.

Приклад 2

У справі "Торговопромислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні", пан Манні вимагав вилучення його особистих даних з реєстру рейтингової компанії. Ці дані пов'язували його з

ліквідацією підприємства з нерухомості, що мало негативний вплив на його репутацію. Європейський Суд вирішив, що "розшифровуючи та зберігаючи таку інформацію в реєстрі та надаючи доступ для ознайомлення у разі необхідності на запит третім сторонам, органи влади, відповідальні за ведення реєстру, здійснюють 'обробку персональних даних', відносно якої вони є 'контролерами'".

Це рішення визначило, що дії органів влади, пов'язані з розкриттям та управлінням інформацією в реєстрі, вважаються обробкою особистих даних, і такі органи виступають в ролі контролерів щодо цієї обробки.

Приклад 3

В сфері трудових відносин роботодавці володіють правом збирати та обробляти дані про своїх працівників, включаючи інформацію про їхні зарплати. Юридичною підставою для цих операцій є трудові договори, які визначають умови зайнятості та взаємодії між сторонами. Однак, коли роботодавці передають інформацію про заробітну плату своїх працівників податковим органам, ця передача також розглядається як "обробка" в контексті Оновленої Конвенції 108 та Загального регламенту з охорони даних.

Важливо зауважити, що для такої передачі даних трудовий договір вже не може вважатися самостійною юридичною підставою. Замість цього, існують потреби в додаткових юридичних підставах для операцій обробки, які призводять до передачі інформації про зарплату працівників до податкових органів. Зазвичай такі юридичні підстави визначаються національними законами про податки. Без наявності відповідних положень та інших юридичних підстав для обробки, така передача персональних даних може вважатися незаконною обробкою відповідно до нормативів захисту даних.

Література

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

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.).

Загальний регламент захисту персональних даних, стаття 4 (1); Оновлена Конвенція 108, стаття 2 (а). 137 Загальний регламент захисту персональних даних, п. 26 преамбули. 138 Там само, стаття 1. 139 Там само, положення 27. Див. також Робоча група «Стаття 29» (2007), Висновок 4/2007 про концепцію персональних даних. РГ 136, від 20 червня 2007 р., с. 22.

Рішення Суду ЄС, об'єднані справи C-92/09 and C-93/09, «“Volker und Markus Schecke GbR” та Хартмут Ейферт проти землі Гессен» (Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen) [ВП], від 9 листопада 2010 р., п. 59.

Суд ЄС, С-101/01, Кримінальне провадження проти Bodil Lindqvist (Criminal proceedings against Bodil Lindqvist), від 6 листопада 2003 р., п. 27.

Рішення Суду ЄС, С-131/12, «“Google Spain SL”, “Google Inc.” проти Іспанського агентства захисту даних (AEPD) та Mario Костеха Гонсалеса» (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González), [ВП], від 13 травня 2014 р.

Рішення ЄСПЛ у справі «Барбулеску проти Румунії» (Bărbulescu v. Romania) [ВП], № 61496/08, від 5 вересня 2017 р., п. 121.

Рішення Суду ЄС, С-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (František Ryneš v. Úřad pro ochranu osobních údajů), від 11 грудня 2014 р., п. 25. 194

Рішення Суду ЄС, С-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні», (Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni), від 9 березня 2017 р., п. 35.

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