ЛУЦЕНКО О. Є.,
кандидатка юридичних наук,
доцентка кафедри трудового права права
(Національний юридичний університет імені Ярослава Мудрого)

УДК 349.2:[342.721:004.056.5]
DOI https://doi.org/10.32842/2078-3736/2023.2.2.20

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ ЗА GDPR

У статті висвітлюється, що Регламент GDPR діє екстериторіально, оскільки поширюється на суб'єктів, що отримують та обробляють персональні дані громадян та резидентів ЄС незалежно від свого місцезнаходження. GDPR не вимагає, аби національні уряди розробляли спеціальні акти для його впровадження, і є безпосередньо обов'язковим до виконання.

Авторка встановила, що відповідно до GDPR, працівник повинен мати можливість чітко розрізняти дані, на обробку/зберігання яких він/вона вільно погоджується та знати цілі, для яких зберігаються його/її дані. Співробітники також повинні бути проінформованими про свої права та тривалість часу, протягом якого дані зберігатимуться, перш ніж можна буде надати згоду. Якщо порушення персональних даних може призвести до високого ризику для прав і свобод фізичних осіб, то роботодавець повинен сповістити про це працівника. GDPR дозволяє державам-членам встановити більш конкретні правила для забезпечення захисту прав і свобод працівників щодо їхніх персональних даних у контексті працевлаштування.

Згідно з Рекомендаціями Ради Європи щодо працевлаштування, персональні дані, зібрані для цілей працевлаштування повинні бути отримані безпосередньо від конкретного працівника. Персональні дані, зібрані для найму, повинні бути обмежені необхідною інформацією, щоб оцінити придатність кандидатів та їхній кар'єрний потенціал. У рекомендації також конкретно згадуються оціночні дані, що стосуються продуктивності або потенціалу окремих працівників. Оціночні дані повинні ґрунтуватися на справедливих та чесних оцінках та не повинні бути образливими у тому, як вони сформульовані. Цього вимагають принципи чесної обробки даних і точності даних.

Конфіденційні персональні дані, зібрані для цілей працевлаштування, можуть оброблятися лише в окремих випадках і відповідно до гарантій, встановлених національним законодавством. Роботодавці можуть запитувати працівників або претендентів на роботу про їхній стан здоров'я лише у разі необхідності. Це може бути для визначення їх придатність до роботи; виконання вимоги профілактичної медицини; захисту життєво важливих інтересів суб'єкта даних або інших працівників і осіб; дозволу надання соціальних пільг; або для надання відповідей на судові запити. Дані про здоров'я можуть не збираються з інших джерел, окрім відповідного працівника, за винятком випадків, коли було отримано чітку та інформовану згоду або коли це передбачено національним законодавством.

Ключові слова: *інформація, захист інформації, персональні дані працівників, трудові правовідносини, працівник, роботодавець.*

Lutsenko O. Ye. Legal regulation of the protection of personal data of employees under the GDPR

The article highlights that the GDPR Regulation applies extraterritorially, as it applies to entities that receive and process the personal data of EU citizens and residents regardless of their location. The GDPR does not require national governments to develop special acts for its implementation and is directly enforceable.

The author established that according to the GDPR, the employee must be able to clearly distinguish the data to which he/she freely consents to the processing/storage and to know the purposes for which his/her data is stored. Employees must also be informed of their rights and the length of time that data will be stored before consent can be given. If a breach of personal data may lead to a high risk for the rights and freedoms of individuals, the employer must notify the employee. The GDPR allows Member States to establish more specific rules to protect employees' rights and freedoms regarding their personal data in the context of employment.

According to the Council of Europe Employment Recommendations, personal data collected for employment purposes must be obtained directly from a specific employee. Personal data collected for recruitment should be limited to the information necessary to assess candidates' suitability and career potential. The recommendation also specifically mentions evaluation data relating to the performance or possibility of individual employees. Evaluation data must be based on fair and honest evaluations and must not be offensive in the way it is worded. This is required by the principles of fair data processing and data accuracy.

Confidential personal data collected for employment purposes may only be processed in specific cases and in accordance with safeguards established by national law. Employers may ask employees or job applicants about their health status only if necessary. This may be to determine their fitness for work; fulfillment of the requirement of preventive medicine; protection of the vital interests of the data subject or other employees and persons; permission to provide social benefits; or to respond to court requests. Health data may not be collected from sources other than the employee concerned, except where express and informed consent has been obtained or when required by national law.

Key words: *information, information protection, employees' personal data, labor relations, employee, employer.*

Вступ. Загальний регламент про захист даних (англ. *General Data Protection Regulation, GDPR; Regulation (EU) 2016/679; далі – GDPR*) [1] – правила, за якими Європейський Парламент, Рада Європейського Союзу та Європейська Комісія посилюють та уніфікують захист персональних даних фізичних осіб. GDPR наслідував положення свого попередника – Директиви 95/46/ЄС Європейського Парламенту від 24.10.1995 р. [2] про захист фізичних осіб при обробці персональних даних і вільне переміщення таких даних. Водночас GDPR суворіший і глибший за Директиву 95/46/ЄС. Принципи й положення Директиви 95/46/ЄС відбиті в Законі України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI [3].

Українські підприємства та фізичні особи-підприємці захищають персональні дані згідно із Законом України «Про захист персональних даних» [3]. Є суб'єкти господарювання, що на додачу до вимог зазначеного Закону мають додержувати й положень GDPR [1]. Це: (1) дочірні підприємства міжнародних компаній в Україні; (2) суб'єкти господарювання, засновані в ЄС українськими підприємствами та громадянами; (3) суб'єкти господарювання, які (а) мають представництво, філію в ЄС; (б) не мають представництва в країнах ЄС, але поставляють товари чи надають послуги фізичним особам в ЄС, у т. ч. на безоплатній основі; (в) моніторять поведінку фізичних осіб в ЄС. Приміром, дотримуватися GDPR мають: (1) дочірні підприємства компаній, що засновані чи діють у країнах ЄС; (2) ІТ-компанії, що розробляють soft-рішення для глобального використання; (3) онлайн-сервіси (інтер-

нет-магазини), що пропонують товари мовами ЄС та приймають оплату в євро; (4) компанії, що доставляють товари фізичним особам у країни ЄС; (5) компанії, що використовують таргетовану рекламу, спрямовану на громадян ЄС; (6) компанії, що моніторять віртуальні дії громадян ЄС, щоб прогнозувати поведінку користувачів товарів чи послуг.

На відміну від Директиви 95/46/ЄС [2], що потребувала імплементації у національне законодавство, Регламент GDPR [1] діє екстериторіально. Він поширюється на суб'єктів, що отримують та обробляють персональні дані громадян та резидентів ЄС незалежно від свого місцезнаходження. GDPR не вимагає, аби національні уряди розробляли спеціальні акти для його впровадження, і є безпосередньо обов'язковим до виконання.

Питання захисту персональних даних працівників є недостатньо дослідженими. Наразі можна назвати лише декількох вчених-трудовиків, які цікавляться цією проблематикою, як-от: А. В. Авраменко [4], І. В. Лагутіна [5], Г. І. Чанишева, Р. І. Чанишев [6], А. М. Чернобай [7]. Не дивлячись на мало дослідженість, все ж проблеми захисту персональних даних працівників гостро стоять, адже процеси європеїзації вимагають переглянути підхід до збирання, обробки, збереження персональних даних працівників.

Постановка завдання. Метою статті є з'ясування особливостей правового регулювання захисту персональних даних працівників за GDPR.

Результати дослідження. У травні місяці 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних («Пакет захисту даних»), який передбачає створення умов забезпечення узгодженої нормативно-правової бази на європейському рівні, що включає наступні документи: (1) Регламент (ЄС) 2016/679 від 27.04.2016 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)» [1]; (2) Директива (ЄС) 2016/680 Європейського Парламенту і Ради від 27.04.2016 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами в цілях запобігання, розслідування, виявлення або переслідування злочинця злочину або виконання кримінальних покарань, а також про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/ПВД» [8]; (3) Директива (ЄС) 2016/681 Європейського Парламенту і Ради від 27.04.2016 р. «Про використання даних записів реєстрації пасажирів (PNR) для профілактики, виявлення, розслідування і судового переслідування злочинів терористичного характеру і тяжкого злочину» [9].

Регламент (ЄС) 2016/679 від 27.04.2016 р. «Загальні Положення про захист даних» (Регламент «GDPR») [1] містить 39 пункту преамбули та 99 статей. Ефективний захист персональних даних на європейській території вимагає зміцнення і встановлення в деталях прав суб'єктів даних і обов'язків тих, хто обробляє і визначає обробку персональних даних, конкретність повноважень для моніторингу виконання правил із захисту персональних даних, а також еквівалентних санкцій за їх порушення в державах-членах ЄС. Це передбачає необхідність правової визначеності та прозорості для всіх малих і середніх підприємств, точності обов'язків і ефективної співпраці між уповноваженими органами держав-членів ЄС. Для забезпечення захисту фізичних осіб і усунення перешкод на шляху потоків персональних даних в рамках ЄС, національні системи обробки та захисту персональних даних повинні бути еквівалентними у всіх державах-членах ЄС [10, с. 47–48].

За визначенням 2016 р., яке сформульовано у Регламенті «GDPR», – «персональні дані означають будь-яку інформацію, що стосується ідентифікованої фізичної особи або фізичної особи, що ідентифікується («суб'єкта даних»); фізична особа, що ідентифікується – це особа, яка може бути ототожнена прямо або опосередковано, зокрема, з ім'ям, ідентифікаційним номером, даними про місцеположення, онлайн ідентифікатором, з одним чи декількома специфічними чинниками для встановлення фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї фізичної особи» [1].

У ньому більш конкретизовано поняття персональних даних та розширений обсяг обов'язків і повноважень відповідних суб'єктів. Генетичні відомості визначені як персональні дані, що відносяться до успадкованих або набутих генетичних характеристик фізич-

ної особи, які є результатом аналізу біологічного зразка, зокрема аналізу хромосом, дезоксирибонуклеїнової (ДНК) або рібонуклеїнової (РНК) кислоти. До відомостей, які стосуються минулого, поточного або майбутнього стану фізичного або психічного здоров'я фізичної особи, додано інформацію щодо надання медичних послуг. Запропоновано визначення «біометричні дані», яке означає особисті дані, одержані в результаті конкретної технічної обробки, пов'язаної з фізичними, фізіологічними або поведінковими характеристиками фізичної особи, що дозволяє підтвердити унікальну ідентифікацію цієї фізичної особи, такі як зображення особи або її дактилоскопічні дані.

Як наголошується у Регламенті «GDPR», захист фізичних осіб у зв'язку з обробкою персональних даних є фундаментальним правом. При цьому, це право не є абсолютним. Воно повинне розглядатися у зв'язку з його функцією в суспільстві і бути збалансованим з іншими основними правами, відповідно до принципу пропорційності, який має бути визначений у базовому законі країни.

Правила Регламенту «GDPR» не застосовуються до обробки персональних даних фізичною особою в ході чисто особистої або побутової діяльності і, таким чином, без зв'язку з професійною або комерційною діяльністю. Особиста або побутова діяльність може включати, зокрема, листування, використання особистої адреси (е-пошта), здійснення онлайн-діяльності у мережах та ін., у відзначеному контексті діяльності. Суб'єкт даних повинен мати можливість передавати свої персональні дані з однієї системи електронної обробки в іншу, без втручання інших осіб.

Регулювання згідно з положеннями Регламенту «GDPR» не застосовується до обробки персональних даних для забезпечення національної безпеки і діяльності правоохоронних органів (для цілей попередження, розслідування), а також до обробки персональних даних державами-членами ЄС по відношенню до загальної зовнішньої політики і політики безпеки ЄС [10, с. 49].

Регламент «GDPR» вводить поняття «контролер» и «процесор», які забезпечують засоби обробки персональних даних. «Контролер» означає фізичну або юридичну особу, державний орган, установу або інший орган, який, поодинці або спільно з іншими, визначає цілі і засоби обробки персональних даних, згідно законодавства. «Процесор» означає фізичну або юридичну особу, державний орган, установу або інший орган, який обробляє персональні дані за дорученням контролера. Також, в компаніях, підприємствах тощо мають бути призначені спеціалісти по захисту даних.

Регламент «GDPR» передбачає наступні санкції, які можуть бути накладені, зокрема: штраф в розмірі від 10.000.000 (або до 2% від річного обігу за попередній фінансовий рік) до 20.000.000 євро (або до 4% від річного обігу попереднього фінансового року).

Безпосереднє застосування Регламенту «GDPR» передбачено з 25 травня 2018 року для всіх держав-членів ЄС, які до вказаного терміну повинні привести свої національні законодавства в повну відповідність з положеннями нових правил [10, с. 50].

У GDPR трудові відносини конкретно згадуються в ст. 9 (2), де зазначено що персональні дані можуть оброблятися під час виконання зобов'язань або здійснення особливих прав контролера або суб'єкта даних у сфері зайнятості. Відповідно до GDPR, працівник повинен мати можливість чітко розрізняти дані, на обробку/зберігання яких він/вона вільно погоджується та знати цілі, для яких зберігаються його/її дані. Співробітники також повинні бути проінформованими про свої права та тривалість часу, протягом якого дані зберігатимуться, перш ніж можна буде надати згоду. Якщо порушення персональних даних може призвести до високого ризику для прав і свобод фізичних осіб, то роботодавець повинен сповістити про це працівника. Стаття 88 GDPR дозволяє державам-членам встановити більш конкретні правила для забезпечення захисту прав і свобод працівників щодо їхніх персональних даних у контексті працевлаштування. Прикладом можна привести справу *Worten* [11], де персональні дані працівника включали дані про робочий час, що охоплювали щоденні періоди роботи та відпочинку, які є персональними даними. У цій справі суд визнав, що національне законодавство може вимагати від роботодавця вести облік робочого

часу, що може стати доступним для національних органів влади, відповідальних за моніторинг умов роботи, однак це вимагає негайно отримати доступ до відповідних персональних даних. Тому для надання громадянину повноваження щодо контролю за законодавством про умови праці слід отримати спеціальний доступ.

Що стосується Ради Європи, Рекомендація щодо даних про зайнятість була видана ще в 1989 році і переглянута в 2015 році [12]. Рекомендація стосується обробки персональних даних з метою працевлаштування як у приватному, так і в державному секторах. Обробка повинна дотримуватися певних принципів і обмежень, таких як принцип прозорості та консультації з представниками працівників перед розміщенням систем моніторингу робочого місця. У рекомендації також зазначено, що роботодавці повинні застосовувати профілактичні заходи, такі як «фільтри», замість того, щоб контролювати використання Інтернету співробітниками.

Огляд найпоширеніших проблем захисту даних, характерних для працевлаштування можна знайти в робочому документі Робочої групи. Так, робоча група проаналізувала значення згоди як правової основи для обробки даних про зайнятість [13]. Було встановлено, що економічний дисбаланс між роботодавцем на запит згоди та працівник, який дає згоду, часто викликають сумніви незалежно від того, чи була згода надана добровільно. Обставини, за яких дається згода, тому слід уважно розглядати при оцінці дійсності згоди в контексті працевлаштування.

Поширеною проблемою захисту даних у сучасному типовому робочому середовищі є обсяг законного моніторингу електронних комунікацій працівників у межах робочого місця. Часто стверджують, що цю проблему можна легко вирішити шляхом заборони приватного використання засобів зв'язку на роботі. Така загальна заборона може однак бути непропорційною і нереалістичною. Рішення ЄСПЛ у справі *Copland* проти Сполученого Королівства та *Bărbulescu* проти Румунії представляють особливий інтерес у контексті цього питання. Так, у справі *Copland* проти Сполученого Королівства [14] телефон, електронна пошта та користування Інтернетом працівника коледжу таємно відстежувалося, щоб переконатися – чи вона (не)надмірно використовувала корпоративний простір коледжу для особистих цілей. ЄСПЛ постановив, що телефонні дзвінки з офісних приміщень охоплювалися поняттями приватного життя та листування. Тому такі дзвінки та електронні листи, надіслані з роботи, а також інформація, отримана з моніторингу персонального використання Інтернету, захищені ст. 8 ЄСПЛ. У справі не існувало положень, які регулювали б обставини, за яких роботодавці можуть контролювати використання працівниками телефон, електронної пошти та Інтернету. Тому втручання не було відповідно до закону. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

У справі *Bărbulescu* проти Румунії [15] заявника було звільнено з роботи за використання Інтернету за місцем роботи в робочий час, порушуючи правила внутрішнього розпорядку. Його роботодавець стежив за його спілкуванням. Записи демонструють, що повідомлення мали суто приватний характер. Визнавши застосовною ст. 8 Конвенції, ЄСПЛ все ж залишив відкритим питання про те, чи відповідали обмежувальні заходи роботодавця «розумним очікуванням конфіденційності», але виявив, що інструкції роботодавця не можуть зменшити приватне соціальне життя на робочому місці до нуля.

Договірним державам надано широку перевагу в оцінці необхідності створення правової бази регулюючих умов, за яких роботодавець може контролювати електронні або інші повідомлення непрофесійного характеру його співробітників на робочому місці. Тим не менш, національні органи влади повинні забезпечити запровадження роботодавцем заходів контролю за листуванням та іншими повідомленнями, незалежно від їх обсягу та тривалості, та супроводжувати це все адекватними та достатніми гарантіями проти зловживання.

Пропорційність і процесуальні гарантії проти свавілля були важливими, і ЄСПЛ визначив ряд факторів, які є актуальними за таких обставин. Сюди входив, серед іншого, ступінь моніторингу з боку роботодавця та ступінь утручання в конфіденційність співробітника; наслідки для працівника; та належність гарантій, які надані. Крім того, вітчизняні

органи влади мають переконатися, що співробітник, комунікація якого контролювався, мав доступ до засобу правового захисту в судовому органі, який має юрисдикцію для визначення, принаймні по суті, як ці критерії були дотримані та чи оскаржувані заходи були законними.

Відтак, у справі *Bărbulescu* проти Румунії [15] ЄСПЛ визнав порушення ст. 8 Конвенції, оскільки національні органи влади не забезпечили належного захисту права заявника на повагу до його приватного життя та листування, і, як наслідок, не вдалося знайти справедливий баланс між інтересами працівника та роботодавця.

Згідно з Рекомендаціями Ради Європи щодо працевлаштування, персональні дані, зібрані для цілей працевлаштування повинні бути отримані безпосередньо від конкретного працівника. Персональні дані, зібрані для найму, повинні бути обмежені необхідною інформацією, щоб оцінити придатність кандидатів та їхній кар'єрний потенціал. У рекомендації також конкретно згадуються оціночні дані, що стосуються продуктивності або потенціалу окремих працівників. Оціночні дані повинні ґрунтуватися на справедливих та чесних оцінках та не повинні бути образливими у тому, як вони сформульовані. Цього вимагають принципи чесної обробки даних і точності даних.

Особливим аспектом законодавства про захист даних у відносинах роботодавець–працівник є роль представників працівників. Такі представники можуть отримувати персональні дані працівників лише в тому обсязі, в якому це необхідно для того, щоб вони могли представляти інтереси працівників або якщо такі дані необхідні для виконання або контролю зобов'язань, передбачених колективними договорами.

Конфіденційні персональні дані, зібрані для цілей працевлаштування, можуть оброблятися лише в окремих випадках і відповідно до гарантій, встановлених національним законодавством. Роботодавці можуть запитувати працівників або претендентів на роботу про їхній стан здоров'я лише у разі необхідності. Це може бути для визначення їх придатність до роботи; виконання вимоги профілактичної медицини; захисту життєво важливих інтересів суб'єкта даних або інших працівників і осіб; дозволу надання соціальних пільг; або для надання відповідей на судові запити. Дані про здоров'я можуть не збираються з інших джерел, окрім відповідного працівника, за винятком випадків, коли було отримано чітку та інформовану згоду або коли це передбачено національним законодавством.

Згідно з Рекомендацією щодо працевлаштування, працівники повинні бути проінформовані про мету обробки їхніх персональних даних, тип зібраних персональних даних, про суб'єктів, яким дані регулярно передаються, а також про ціль і право можливого розкриття інформації. Електронний зв'язок доступний лише на робочому місці з міркувань безпеки чи з інших законних причин, а також такий доступ дозволяється лише після того, як працівники були поінформовані про те, що роботодавець міг зробити доступ до цього виду спілкування.

Працівники повинні мати право доступу до даних про свою роботу, а також право на виправлення або знищення, та оскаржити рішення суду. Проте ці права можуть бути тимчасово обмеженими з метою внутрішніх розслідувань. Якщо працівнику відмовлено у доступі, то виправлення або видалення особистих даних про роботу, має передбачати національне законодавство, зокрема встановлюючи відповідні процедури оскарження такої відмови [16, с. 330–335].

Висновки. Відповідно до GDPR, працівник повинен мати можливість чітко розрізняти дані, на обробку/зберігання яких він/вона вільно погоджується та знати цілі, для яких зберігаються його/її дані. Співробітники також повинні бути проінформованими про свої права та тривалість часу, протягом якого дані зберігатимуться, перш ніж можна буде надати згоду. Якщо порушення персональних даних може призвести до високого ризику для прав і свобод фізичних осіб, то роботодавець повинен сповістити про це працівника. GDPR дозволяє державам-членам встановити більш конкретні правила для забезпечення захисту прав і свобод працівників щодо їхніх персональних даних у контексті працевлаштування.

Згідно з Рекомендаціями Ради Європи щодо працевлаштування, персональні дані, зібрані для цілей працевлаштування повинні бути отримані безпосередньо від конкретного працівника. Персональні дані, зібрані для найму, повинні бути обмежені необхідною інфор-

мацією, щоб оцінити придатність кандидатів та їхній кар'єрний потенціал. У рекомендації також конкретно згадуються оціночні дані, що стосуються продуктивності або потенціалу окремих працівників. Оціночні дані повинні ґрунтуватися на справедливих та чесних оцінках та не повинні бути образливими у тому, як вони сформульовані. Цього вимагають принципи чесної обробки даних і точності даних.

Конфіденційні персональні дані, зібрані для цілей працевлаштування, можуть оброблятися лише в окремих випадках і відповідно до гарантій, встановлених національним законодавством. Роботодавці можуть запитувати працівників або претендентів на роботу про їхній стан здоров'я лише у разі необхідності. Це може бути для визначення їх придатність до роботи; виконання вимоги профілактичної медицини; захисту життєво важливих інтересів суб'єкта даних або інших працівників і осіб; дозволу надання соціальних пільг; або для надання відповідей на судові запити. Дані про здоров'я можуть не збираються з інших джерел, окрім відповідного працівника, за винятком випадків, коли було отримано чітку та інформовану згоду або коли це передбачено національним законодавством.

Список використаних джерел:

1. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglament (EU) 2016/679 of the European Parlament and of the Council, of 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата звернення 05.03.2023).

2. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»: директива Європейського Союзу від 24.10.1995 № 95/46/ЄС URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення 09.03.2023).

3. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

4. Авраменко А.В. Правове регулювання відносин щодо обігу та захисту персональних даних працівника в трудовому праві України: дис. канд.юрид.наук: 12.00.05. Київ, 2019. 228 с.

5. Лагутіна І.В. Особисті немайнові трудові права працівників у системі трудових прав : монографія. Одеса: Фенікс, 2014. 428 с.

6. Чанишева Г.І., Чанишев Р.І. Право на інформацію за трудовим законодавством України : монографія. Одеса: Фенікс, 2012. 196 с.

7. Чернобай А.М. Правові засоби захисту персональних даних працівника : дис. … канд. юрид. наук: 12.00.05. Одеса, 2006. 200 с.

8. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA : Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 (дата звернення 05.03.2023).

9. On the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime : Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L0681 (дата звернення 05.03.2023)

10. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. № 3(18). 2016. С. 45–57.

11. CJEU, C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), 30 May 2013, para. 19 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1512486680719&uri=CELEX:62012CJ0342 (дата звернення 09.03.2023).

12. Council of Europe, Committee of Ministers (2015), Recommendation Rec(2015)5 to member states on the processing of personal data in the context of employment, April 2015. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

13. Article 29 Working Party (2005), Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 November 2005. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm (дата звернення 09.03.2023)

14. ECtHR, Copland v. the United Kingdom, No. 62617/00, 3 April 2007. URL: https://uk.practicallaw.thomsonreuters.com/1-369-8081?transitionType=Default&contextData=(sc.Default)&firstPage=true (дата звернення 09.03.2023)

15. ECtHR, Bărbulescu v. Romania [GC], No. 61496/08, 5 September 2017, para. 121. URL: https://hudoc.echr.coe.int/fre#{“sort”:[“kpdate%20Descending”],”documentcollectionid2”:[“JUDGMENTS”,”DECISIONS”],”itemid”:[“001-177082”]} (дата звернення 09.03.2023)

16. Handbook on European data protection law. Luxembourg: Publications Office of the European Union, 2018. 402 p.