**НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ**
**ІМЕНІ ЯРОСЛАВА МУДРОГО**
**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

*Кваліфікаційна наукова праця*
*на правах рукопису*

**МИХАЙЛИК АЛІНА СЕРГІЇВНА**

***УДК 349.2:[342.721:004.056.5]***

# ДИСЕРТАЦІЯ
# ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

081 «Право»

08 «Право»

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ А. С. Михайлик

Науковий керівник –
**Ярошенко Олег Миколайович,**
доктор юридичних наук, професор,
член-кореспондент НАПрН України,
заслужений діяч науки і техніки України

**Харків – 2023**

# АНОТАЦІЯ

***Михайлик А. С.*** Захист персональних даних працівників в умовах цифрової трансформації. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». – Національний юридичний університет імені Ярослава Мудрого, Міністерство освіти і науки України, Харків, 2023.

У дисертації доведено, що захист персональних даних працівника є елементом трудових правовідносин, а також з метою забезпечення їх одноманітного правового режиму, захист персональних даних працівника слід розглядати як самостійний інститут трудового права. Адже суспільні відносини, пов'язані із захистом персональних даних працівника, є окремими видами правовідносин у сфері праці, які можуть як передувати (надання інформації в ході працевлаштування у певного роботодавця), супроводжувати (приміром, ухвалення рішення про просуванні працівника по службі), так і випливати з трудових правовідносин (приміром, розголошення комерційної таємниці), специфіка яких пов'язана з ключовими суб'єктами трудового права – працівниками та роботодавцями.

Авторкою визначено, що персональні дані працівника – це інформація, яка стосується загальних даних про особу працівника та/або кандидата на посаду, професійної кваліфікації працівника/кандидата на посаду, ділових, професійних якостей, а також інформація щодо спеціальних вимог, які можуть встановлюватися законодавством до працівників/кандидатів на посаду у зв'язку з характером їх роботи (приміром, заповнення декларації про доходи, проходження спеціальної перевірки тощо). Тобто персональні дані працівника мають забезпечувати ідентифікацію його/її не тільки і не стільки як людину, а насамперед як працівника. Це означає, що персональні дані працівника та претендента на посаду – це, в першу чергу, інформація, що стосується професійної кваліфікації, ділових, професійних якостей та відповідності працівника та претендента на посаду вимогам, які можуть бути до нього пред'явлені у зв'язку з характером роботи.

Класифікація персональних даних працівника, в аспекті їх збору, обробки та правового режиму використання має провадитися на такі групи:

а) загальні «анкетні» персональні дані (відомості про прізвище, ім’я, по батькові, дата та місце народження, паспортні дані, відомості про освіту, про професійні навички, відомості про «історію» трудової діяльності тощо);

б) спеціальні персональні дані: расова, національна приналежність, політичні погляди, релігійні чи філософські переконання, стан здоров'я, приватне життя. Збір та обробка цих персональних даних має бути заборонена для роботодавця;

в) персональні дані обмеженого доступу, до яких слід віднести відомості про усиновлення, судимість, участі у кримінальному судочинстві як підозрюваного, наданої чи прийнятої фінансової допомоги, чи послуг, декларація про доходи, результати спеціальної перевірки тощо;

г) біометричні персональні дані – відомості, що містять характеристики фізіологічних та біологічних особливостей людини, що дають можливість встановлення її особистості. Ці дані є «чутливими даними» і мають особливий правовий режим захисту. Для їх обробки роботодавцем потрібне спеціальне погодження Уповноваженим ВРУ.

У дисертації обґрунтовано, що специфіка захисту персональних даних осіб, які здійснюють свою професійну діяльність на підставі трудового договору, проявляється, перш за все, в тому, що основні вимоги щодо обробки персональних даних працівника встановлюються нормами законодавства, а порядок здійснення окремих операцій з персональними даними працівника (збір, зберігання, використання, поширення) може деталізуватися у локальних правових актах. Обов'язок не розголошувати персональні дані також може бути передбачений законами та підзаконними актами для окремих категорій осіб, наприклад, для державних службовців.

Виокремлено чотири послідовні дії для реалізації механізму захисту персональних даних працівника: а) визначити технічні та організаційні заходи, які треба вжити; б) призначити відповідального за обробку і захист персональних даних. Якщо роботодавець — орган влади, ОМС чи

підприємство, що обробляє чутливі персональні дані, призначайте відповідального обов’язкового. В інших випадках — за рішенням керівника підприємства; в) розробити Положення про порядок обробки та захисту персональних даних (Додаток А); г) отримати зобов’язання про нерозголошення персональних даних від працівників, які стикаються під час роботи з персональними даними інших осіб. Зареєструвати отримані зобов’язання в Журналі реєстрації зобов’язань про нерозголошення персональних даних.

Доведено, що надання інформації про персональні дані працівника на телефонний запит є неправомірним, позаяк таку інформацію слід надавати тільки за письмовими запитами та за згодою працівника, яку він/вона надав(ла), або володільцю його персональних даних, або запитувачу. Оскільки якщо передавати таку інформацію телефоном, то роботодавець ризикує, адже працівник може поскаржитися омбудсмену на те, що роботодавець незаконно поширив його/її персональні дані, а як наслідок роботодавець може отримати штраф.

У дисертації встановлено, що ані КЗпП України, ані жодним законом України (у т. ч. законодавством про захист персональних даних) не передбачено обов’язку або можливості надання закладом охорони здоров’я або правоохоронним органом відомостей про події або явища, що відбуваються у житті працівника (звернення за медичною допомогою, перебування на лікуванні, участь в досудовому розслідуванні у якості свідка тощо), на запит роботодавця. Тому відмова офіційних органів у наданні інформації про стан здоров’я працівника, про його звернення чи не звернення до медичних закладів, є цілком правомірною. Інформація про стан здоров'я працівника може бути необхідною роботодавцю для вирішення питання про можливість допуску того чи іншого працівника до виконання певної роботи, але у такому випадку цю інформацію роботодавець має отримати виключно від самого працівника.

У випадку розміщення інформації про працівників на корпоративному сайті підприємства, установи чи організації, а також у соціальних мережах, то

роботодавець повинен отримати згоду працівника та визначити, де і скільки зберігатимете згоди працівників. Допоки інформація про працівника є на сайті чи в соцмережах, то слід зберігати згоду на обробку персональних даних. Якщо підприємство хоче використовувати відомості щодо працівника як власну конкурентну перевагу, для підвищення ділової репутації, просування товарів чи послуг в інтернеті, соцмережах, то згода на обробку персональних даних також потрібна.

Авторка встановила, що чинне законодавство не забороняє запроваджувати допуск працівників на підприємство шляхом обробки відбитків пальців, але процедура запровадження — вельми клопітка. Слід врахувати вимоги законодавства у сфері захисту персональних даних, адже відбитки пальців належить до персональних біометричних даних. Такі дані вважають особливо чутливими, адже їх обробка становить особливий ризик для прав і свобод людини. Тому роботодавець має отримати від кожного працівника згоду на обробку персональних даних у вигляді обробки відбитків пальців. Якщо хоча б один працівник не надасть згоду на обробку відбитків пальців, то запровадити обробку біометричних даних роботодавець не зможе.

Особливості роботи з автоматизованою базою персональних даних як набору даних, що ідентифікують працівника та кандидата на посаду, до яких застосовується автоматична обробка: роботодавець зобов'язаний забезпечити цільову відповідність, точність отримання та обробки даних, захист від несанкціонованого використання, посилений режим охорони особливих категорій відомостей (про національну приналежність, погляди та переконаннях, здоров'я та інтимного життя, судимості та ін.).

ATS (*Applicant tracking system*) — це програмне забезпечення, яке дозволяє працювати з кадровими процесами в компанії в електронному вигляді. Такі автоматизовані системи пропонують численні переваги малому та середньому бізнесу, роблячи їхні завдання з підбору та найму персоналу набагато ефективнішими. Вибір правильної платформи все ще викликає багато труднощів, адже всі організації різні та мають свої власні складності, однак знання ключових характеристик і завчасне визначення конкретних вимог

роблять вибір ATS набагато менш громіздким. Автоматизовані системи управління персоналом мають низку переваг, зокрема: мобільність, відповідність даних, візуалізація даних, формування бази кандидатів та співробітників та високий ступінь захисту інформації.

Із відносинами з автоматизованої обробки персональних даних пов'язане спостереження за працівником на робочому місці, прослуховування його телефонних розмов та здійснення нагляду в інших формах. Приховане чи явне спостереження працівниками є поширеною практикою, яку здійснюють вітчизняні роботодавці. Однак брак правових норм у цій сфері нерідко призводить до обмеження та порушення прав та законних інтересів працівників. Слід закріпити, що спостереження за працівником можливе лише у випадках, необхідних для забезпечення збереження майна роботодавцю, усунення загроз здоров'ю та суспільної безпеки. Якщо працівник піддається спостереженню на робочому місці, то він має бути попередньо поінформований про причини спостереження, режим часу спостереження, використовувані методи та засоби збору інформації. Разом з цим, персональні дані, отримані внаслідок спостереження за працівником, не повинні бути єдиною підставою для висновку про продуктивність та якість праці працівника. Роботодавець повинен вжити всі можливі заходи для того, щоб звести до мінімуму «вторгнення» в особисте життя працівника.

Практичне значення одержаних результатів полягає в тому, що положення й висновки дисертації можуть бути використані:

– у науково-дослідницькій діяльності – з метою подальшого вивчення й розкриття порушеної проблематики, вдосконалення правового регулювання захисту персональних даних працівників;

– у навчальному процесі – при викладанні навчальної дисципліни «Трудове право», при написанні відповідних розділів підручників, навчальних посібників, курсів лекцій, а також при підготовці студентами наукових робіт;

– у правотворчості – у процесі реформування й удосконалення чинного трудового законодавства щодо правової регламентації захисту персональних даних працівників відповідно до наданих пропозицій;

– у правозастосуванні – при оперуванні наведеними висновками, рекомендаціями і пропозиціями в діяльності органів державної влади України.

***Ключові слова*:** інформація, захист інформації, конфіденційна інформація, персональні дані працівників, інформація, яка подається при прийнятті на роботу, трудові правовідносин, працівник, роботодавець, трудовий договір, збір та облік документів при прийнятті на роботу.

## SUMMARY

***Mykhailyk A. S.*** Protection of employees' personal data in digital transformation conditions. – Qualifying scientific work on the rights of manuscripts.

Thesis for the philosophy doctor degree in specialty 081 «Law». – Yaroslav Mudryi National Law University, Ministry of Education and Science of Ukraine, Kharkiv, 2023.

It has proved that the protection of the employee's personal data is an element of labour relations, and in order to ensure their uniform legal regime, the protection of the employee's personal data should be considered an independent institution of labour law. After all, social relations related to the protection of an employee's personal data are separate types of legal relations in the field of labour, which can both precede (providing information during employment with a certain employer), accompany (for example, making a decision on the promotion of an employee), and arise from labour relations (for example, the disclosure of commercial secrets), the specifics of which are related to the key subjects of labour law – employees and employers.

The author has defined that the personal data of an employee is information related to general data about the identity of the employee and/or a candidate for the position, the professional qualifications of the employee/ a candidate for the position, business, professional qualities, as well as information about special requirements that may be established by legislation to employees/ a candidates for the position in connection with the nature of their work (for example, filling out the

income declaration, passing a special check, etc.). That is, the employee's personal data should ensure his/her identification not only and not so much as a person, but primarily as an employee. This means that the personal data of the employee and applicant for the position is, first of all, information related to professional qualifications, business, professional qualities and compliance of the employee and applicant for the position with the requirements that may be presented to him in connection with the nature of the work.

The classification of the employee's personal data, in terms of their collection, processing and legal regime of use, should be carried out into the following groups:

a) general “questionnaire” personal data (information about the surname, first name, patronymic, date and place of birth, passport data, information about educational professional skills, information about the “history” of labour activity, etc.);

b) special personal data: race, nationality, political views, religious or philosophical beliefs, state of health, private life. The collection and processing of this personal data must be prohibited for the employer;

c) personal data with limited access, which should include information about adoption, criminal record, participation in criminal proceedings as a suspect, financial assistance or services provided or received, income declaration, results of a special check, etc.;

d) biometric personal data – information containing the characteristics of a person's physiological and biological characteristics, which make it possible to establish his personality. This data is “sensitive data” and has a special legal protection regime. Their processing by the employer requires special approval by the Commissioner of the VRU.

The thesis substantiates that the specificity of the protection of personal data of persons who carry out their professional activities on the basis of an employment contract is manifested, first of all, in the fact that the basic requirements for the processing of an employee's personal data are established by legislation, and the procedure for carrying out individual operations with personal data employee (collection, storage, use, distribution) can be detailed in local legal acts. The

obligation not to disclose personal data may also be provided by laws and by-laws for certain categories of persons, for example, for civil servants.

Four consecutive actions for the implementation of the mechanism for the protection of the employee's personal data are identified: a) determine the technical and organizational measures that must be taken; b) appoint a person responsible for the processing and protection of personal data. If the employer is a government body, local government or enterprise that processes sensitive personal data, appoint a responsible person. In other cases, according to the decision of the head of the enterprise; c) develop Regulations on the procedure for processing and protecting personal data (Appendix A); d) obtain an obligation not to disclose personal data from employees who come into contact with personal data of other persons during work. Register the obligations received in the Journal of registration of obligations about non-disclosure of personal data.

It has been proven that the provision of information about an employee's personal data upon a telephone request is unlawful, as such information should be provided only upon written requests and with the employee's consent, which he/she has provided, or to the owner of his/her personal data, or to the requester. Because if such information is transmitted over the phone, the employer is at risk, because the employee can complain to the ombudsman that the employer has illegally shared his/her personal data, and as a result, the employer can receive a fine.

It has established that neither the Labour Code of Ukraine nor any law of Ukraine (including the legislation on the protection of personal data) provides for the obligation or the possibility of providing a healthcare institution or a law enforcement agency with information about events or phenomena that occur in the employee's life (seeking medical help, receiving treatment, participating in a pre-trial investigation as a witness, etc.), at the employer's request. Therefore, the refusal of official bodies to provide information about the employee's state of health, whether or not he goes to medical facilities, is completely legitimate. Information about an employee's state of health may be necessary for the employer to decide on the possibility of allowing this or that employee to perform certain work, but in this case the employer must obtain this information exclusively from the employee

himself. In the case of posting information about employees on the corporate website of an enterprise, institution or organization, as well as on social networks, the employer must obtain the employee's consent and determine where and how long the employee's consent will be stored. As long as information about the employee is available on the website or in social networks, consent to the processing of personal data should be kept. If the company wants to use information about the employee as its own competitive advantage, to improve its business reputation, promote goods or services on the Internet, social networks, then consent to the processing of personal data is also required.

The author established that the current legislation does not prohibit the introduction of employee admission to the enterprise by processing fingerprints, but the implementation procedure is very troublesome. The requirements of the legislation in the field of personal data protection should be taken into account, because fingerprints belong to personal biometric data. Such data are considered particularly sensitive, because their processing poses a particular risk to human rights and freedoms. Therefore, the employer must obtain consent from each employee for the processing of personal data in the form of fingerprint processing. If at least one employee does not consent to the processing of fingerprints, the employer will not be able to implement the processing of biometric data. Peculiarities of working with an automated database of personal data as a set of data identifying an employee and a candidate for a position, to which automatic processing is applied: the employer is obliged to ensure target compliance, the accuracy of data acquisition and processing, protection against unauthorized use, enhanced protection regime for special categories of information (about nationality, views and beliefs, health and intimate life, criminal record, etc.).

ATS (*Applicant tracking system*) is software that allows you to work with personnel processes in the company electronically. Such automated systems offer numerous benefits to small and medium-sized businesses, making their recruitment and staffing tasks much more efficient. Choosing the right platform is still a challenge as all organizations are different and have their own complexities, but knowing the key features and identifying specific requirements early on makes

choosing an ATS much less cumbersome. Automated personnel management systems have a number of advantages, including: mobility, data compliance, data visualization, candidate and employee database formation, and a high degree of information protection.

Monitoring of the employee at the workplace, listening to his telephone conversations and carrying out supervision in other forms is connected with the relationship of automated processing of personal data. Covert or overt surveillance of employees is a common practice carried out by domestic employers. However, the lack of legal norms in this area often leads to restrictions and violations of the rights and legitimate interests of employees. It should be established that surveillance of the employee is possible only in cases necessary to ensure the preservation of the employer's property, elimination of threats to health and public safety. If the employee is subject to observation at the workplace, he must be informed in advance about the reasons for observation, the mode of observation time, the methods used and the means of information collection. At the same time, personal data obtained as a result of observing an employee should not be the only basis for a conclusion about the productivity and quality of the employee's work. The employer must take all possible measures to minimize the "intrusion" into the employee's personal life.

The practical significance of the obtained results is that the provisions and conclusions of the dissertation can be used:

– in scientific and research activities – for the purpose of further study and disclosure of the raised issues, improvement of the legal regulation of the protection of personal data of employees;

– in the educational process – when teaching the academic discipline “Labour Law”, when writing relevant sections of textbooks, study guides, lecture courses, as well as when students prepare scientific papers;

– in law-making – in the process of reforming and improving the current labour legislation regarding the legal regulation of the protection of personal data of employees in accordance with the provided proposals;

– in law enforcement – when operating the given conclusions, recommendations and proposals in the activities of the state authorities of Ukraine.

***Key words:*** information, information protection, confidential information, employees' personal data, information submitted when hiring, employment relationship, employee, employer, employment contract, collection and accounting of documents when hiring.

# СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

*Наукові праці, в яких відображені основні результати дослідження:*

1. Михайлик А. С. Сучасний стан та проблеми захисту персональних даних працівників в Україні в умовах цифрової трансформації. *Соціальне право*. 2021. № 4. С. 200–207.
2. Михайлик А. С. Гарантії захисту персональних даних працівників в Україні: законодавче забезпечення. *Правові новели*. 2022. № 16. С. 29–34.
3. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. *Науковий вісник Ужгородського національного університету. Серія "Право"*. 2022. Вип. 72 (2). С. 82–87.
4. Mykhailyk A. S. International legal standards in the field of protection of personal data of employees. *The scientific heritage*. 2022. № 95(95). P. 35–38.

*Наукові праці, в яких засвідчено апробацію матеріалів дослідження:*

1. Михайлик А. С. Щодо захисту персональних даних працівників. *Правові виклики сучасності: захист прав людини в умовах пандемії* : матеріали ІІ міжнар. наук.-практ. онлайн конф. (м. Чернівці, 22 жовт. 2021 р.) / [редкол.: Н. Д. Гетьманцева (гол.), О. В. Кіріяк (відп. секр.) та ін.]. Чернівці : Чернівец. нац. ун-т ім. Ю. Федьковича, 2021. С. 238–239.
2. Михайлик А. С. Забезпечення захисту персональних даних працівників: невирішені питання. *Правове забезпечення соціальної безпеки в умовах євроінтеграційних процесів* : тези допов. учасн. ІІІ міжнар. наук.-практ. конф. (м. Київ, 26 листоп. 2021 р.) / за ред. М. І. Іншина, М. Б. Мельник. Київ : ФОП Маслаков, 2021. С. 166–168.
3. Михайлик А. С. Щодо законодавчого забезпечення захисту персональних даних працівників в Україні відповідно до міжнародних стандартів. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття»* (до 25-річчя Національного університету «Одеська юридична

академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали міжнар. наук.-практ. конф. (м. Одеса, 17 черв. 2022 р.) / за заг. ред. С. В. Ківалова. Одеса : Вид. дім «Гельветика», 2022. Т. 1. С. 598–601.

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GDPR – *General Data Protection Regulation* / Загальний регламент про захист даних

АМКУ – Антимонопольний комітет України

АТ – акціонерне товариство

ВРУ – Верховна Рада України

ВС – Верховний Суд

ДМС – Державна міграційна служба України

ДСЗ – Державна служба зайнятості України

ДФС – Державна фіскальна служба України

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

Закон України № 2297 – Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI

ЗПД – захист персональних даних

ЗСУ – Збройні Сили України

ЗУ – Закон України

ІКТ – інформаційно-телекомунікаційні технології

КЗпП України – Кодекс законів про працю України

КМУ – Кабінет Міністрів України

КП – Класифікатор професій

КСУ – Конституційний Суд України

КУпАП – Кодекс України про адміністративні правопорушення

МВС – Міністерство внутрішніх справ

МДА – місцеві державні адміністрації

МОМ – Міжнародна організація міграції

МОН – Міністерство освіти і науки України

МОП – Міжнародна організація праці

НБУ – Національний банк України

нмдг – неоподаткований мінімум доходів громадян

ОМС – органи місцевого самоврядування

ООН – Організація Об’єднаних Націй

ПД – персональні дані

Порядок контролю – Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних

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

ПФУ – Пенсійний Фонд України

РДА – районні державні адміністрації

РЄ – Рада Європи

СЄС – Суд Європейського Союзу

США – Сполучені Штати Америки

Типовий порядок обробки ПД – Типовий порядок обробки персональних даних

ТНК – транснаціональні корпорації

ТОВ – товариство з обмеженою відповідальністю

ТЦК та СП – територіальні центри комплектування та соціальної підтримки

Уповноважений ВРУ/ омбудсмен – Уповноважений Верховної Ради України з прав людини

УСЗН – Управління соціального захисту населення

ФРН – Федеративна Республіка Німеччини

ЦК України – Цивільний кодекс України

члени КПРС – члени комуністичної партії Радянського Союзу

# ВСТУП

**Обґрунтування вибору теми дослідження.** Поява та розвиток економіки, заснованої на технічних та технологічних знаннях, разом із зростанням інформаційно-комунікативного прогресу і посиленням ролі людського капіталу здійснюють неабиякий вплив на трудове життя. Хоча ці зміни є позитивними з точки зору продуктивності та конкурентоспроможності, але вони також викликають певну кількість проблем і ризиків. Інформація та знання стали вирішальними факторами постіндустріального ринку праці. Саме тому нині трудові відносини характеризуються збільшенням значних потоків інформації. Це, зокрема, відбувається під впливом нового менеджменту з управління людськими ресурсами, в якому саме працівник визначається ключовим у досягненні успіху в бізнесі.

Більше того, глобалізація економіки, збільшення міжнародних корпоративних злиттів і розгортання інформаційного суспільства, яке рухається технологічними інноваціями, збільшило потреби в інформації як компаній, так і робочої сили.

Трудові відносини особливо чутливі до інформації, вони найбільше пов’язані з питаннями регулювання інформації, включаючи захист персональних даних працівників. Саме тому одне з питань, яке вийшло на перший план і нині є предметом активних науково-прикладних дискусій, законотворчості та досліджень на міжнародному, європейському та національному рівнях є захист персональних даних працівників.

Величезна кількість трудових завдань, що виконуються працівниками регулярно на роботі, вже передбачає збір та обробку персональних даних на всіх етапах трудової діяльності. Сучасні розробки в управлінні людськими ресурсами, спрямовані на підвищення ролі людського капіталу компаній, як в організації роботи, так і у використанні інформаційно-комунікаційних технологій, а тому на робочому місці постійно ведуться збір та обробка персональних даних працівників. А ефективне використання технологічних

пристроїв сприяє і, ймовірно, й надалі сприятиме «вторгненням» до простору працівників.

На цьому фоні, з одного боку, зростає усвідомлення важливості фундаментальних прав працівника перш за все як людини, зокрема, права на приватне життя та на захист персональних даних, а з іншого боку, заглиблюється усвідомлення ролі якості виконуваної роботи як рушійної сили для процвітання економіки, збільшення кількості кращих робочих місць та створення сприятливого середовища для інклюзивного суспільства.

У зв'язку з наведеним, наука трудового права та практика потребує новітнього дослідження із захисту персональних даних працівників, зокрема з'ясування сутності та видів персональних даних працівників, конфіденційних даних, а також виявлення особливостей моніторингу та нагляду за працівниками на роботі. Саме тому ця дисертація покликана пролити світло на складну нормативну базу, яка характеризується взаємодією правових положень у різних галузях права та спрямована на надання інструментів для кращого розуміння існуючої ситуації, ідентифікації викликів у майбутньому та виробленню науково-виважених пропозицій та рекомендацій для удосконалення правового регулювання захисту персональних даних працівників.

Науково-теоретичним підґрунтям цього дослідження послужили праці вчених, як-от: Ф. А. Абаєва, А. В. Авраменко, Е. Н. Бондаренко, Д. В. Іванова, А. В. Дворецкого, М. В. Різак, Р. І. Чанишева, Г. І. Чанишевої, А. М. Чернобая, А. О. Щербини та ін. На жаль, ученими у сфері трудового права розкривалися лише окремі питання персональних даних працівників, а ось комплексно питання захисту персонального захисту персональних даних не вивчалися. З урахуванням цього, трудо-правові аспекти захисту персональних даних працівників потребують нагального всебічного наукового дослідження, яке розкривало б сутність та особливості захисту персональних даних працівників та надало б пропозиції для удосконалення правового регулювання цих питань.

**Зв'язок роботи з науковими програмами, планами, темами.** Дисертаційна робота, виконана на кафедрі трудового права Національного

юридичного університету імені Ярослава Мудрого, спрямована на виконання Стратегії сталого розвитку «Україна – 2020», схваленої Указом Президента України від 12 січня 2015 р. за № 5/2015, і Стратегії розвитку наукових досліджень НАПрН України на 2016–2020 роки, схваленої постановою загальних зборів НАПрН України від 3 березня 2016 р., Пріоритетних напрямів розвитку правової науки на 2016–2020 роки, затверджених постановою загальних зборів НАПрН України від 3 березня 2016 р. і цільової комплексної програми Національного юридичного університету імені Ярослава Мудрого «Проблеми вдосконалення правового регулювання відносин у сфері праці та соціального захисту» (номер державної реєстрації 0111U000960).

**Мета й завдання дослідження.** Мета наукової роботи полягає в тому, щоб на підставі аналізу чинного законодавства України, практики його застосування й теоретичного осмислення наукових праць вітчизняних і зарубіжних учених у відповідних галузях знань з'ясувати особливості захисту персональних даних працівників, а також сформулювати висновки, пропозиції та рекомендації, спрямовані на вдосконалення правового регулювання захисту персональних даних працівників.

Для досягнення цієї мети були поставлені такі завдання:

– виявити основні концептуальні підходи до дослідження механізмів забезпечення захисту персональних даних працівників;

– розкрити зміст поняття персональних даних працівників;

– показати особливості міжнародної практики захисту персональних даних на підприємствах;

– виявити сучасний стан, становлення та розвиток державних механізмів забезпечення захисту персональних даних працівників;

– установити шляхи вдосконалення захисту персональних даних працівників та їх правового закріплення;

– з'ясувати заходи забезпечення захисту персональних даних працівників;

– навести гарантії захисту персональних даних працівників в Україні;

– спрогнозувати перспективні напрями вдосконалення і розвитку забезпечення захисту персональних даних працівників в Україні.

*Об'єкт дослідження* становлять правовідносини, які виникають у зв'язку з захистом персональних даних працівників.

*Предметом дослідження* є захист персональних даних працівників в умовах цифрової трансформації.

**Методи дослідження.** Для комплексного розкриття тематики дослідження, досягнення неупередженого наукового результату і формулювання відповідних висновків використано низку загальнонаукових і спеціальних методів пізнання. Як основу для наукових пошуків взято діалектичний метод, що сприяв всебічному вивченню процесів збору, обробки та захисту персональних даних працівників в умовах цифрової трансформації в їх взаємозв'язку і взаємозумовленості, що дозволило розкрити сучасний стан розглядуваного предмета (підрозділи 1.1; 1.2). Функціональний метод став у нагоді при з'ясуванні внутрішньосистемних, міжсистемних і зовнішньосистемних зв'язків захисту персональних даних працівників (підрозділи 2.1; 2.2). Формально-логічний метод обрано у процесі критичного аналізу чинного трудового законодавства в питаннях, що стосуються правової регламентації захисту персональних даних працівників в умовах цифрової трансформації, що допомогло розробленню пропозицій з удосконалення законодавства про працю, а також здійсненню дослідження судової практики як емпіричної бази для наукових пошуків (підрозділи 2.1; 2.2; 3.1; 3.2). Метод компаративістики задіяно з метою аналізу зарубіжного досвіду правового регулювання захисту персональних даних працівників (підрозділи 1.3). У дисертації знайшли відбиття також деякі інші наукові методи.

Основні висновки, положення й результати наукових пошуків ґрунтуються на поглибленому вивченні чинного вітчизняного трудового законодавства, судової практики і юридичної (наукової й навчальної) літератури, що стосується порушених у роботі питань.

**Наукова новизна одержаних результатів** полягає в тому, що дисертація є першою у вітчизняній науці трудового права комплексною

теоретико-прикладною працею, в якій на підставі детального опрацювання наукових праць учених у різних сферах знань, зокрема, у галузі трудового права, системного аналізу національного законодавства, зарубіжного і міжнародного досвіду, проведено дослідження захисту персональних даних працівників в умовах цифрової трансформації. Це дозволило обґрунтувати низку новітніх теоретичних та прикладних положень, підготувати науково-прикладні рекомендації та пропозиції з досліджуваних питань. Новизна поданого на захист рукопису реалізується в нижче наведених науково-теоретичних положеннях, висновках і пропозиціях.

*Уперше:*

– виокремлено чотири стадії (послідовних дій) для реалізації механізму захисту персональних даних працівника: а) визначити технічні та організаційні заходи, які треба вжити; б) призначити відповідального за обробку і захист персональних даних; в) розробити Положення про порядок обробки та захисту персональних даних; г) отримати зобов’язання про нерозголошення персональних даних від працівників, які стикаються під час роботи з персональними даними інших осіб;

– висловлено позицію, що у випадку розміщення інформації про працівників на корпоративному сайті підприємства, установи чи організації, а також у соціальних мережах, роботодавець повинен отримати згоду працівника та визначити період протягом якого зберігатиме згоди працівників;

– арґументовано, що допуск працівників на підприємство шляхом обробки відбитків пальців є допустимою, але слід врахувати вимоги законодавства у сфері захисту персональних даних, адже відбитки пальців належить до персональних біометричних даних, а ці дані «особливо чутливими», адже їх обробка становить особливий ризик для прав і свобод людини. Тому роботодавець має отримати від кожного працівника згоду на обробку персональних даних у вигляді обробки відбитків пальців. Якщо хоча б один працівник не надасть згоду на обробку відбитків пальців, то запровадити обробку біометричних даних роботодавець не зможе;

– доведено, що Автоматизовані системи управління персоналом ATS (*Applicant tracking system*) мають низку переваг, зокрема: мобільність, відповідність даних, візуалізація даних, формування бази кандидатів та співробітників та високий ступінь захисту інформації, а тому їх використання потребує нормативного регламентування з метою високого ступеня захисту персональних даних працівників;

– установлено, що заклад охорони здоров’я не має ані обов’язку, ані права надання відомостей про події або явища, що відбуваються у житті працівника (звернення за медичною допомогою, перебування на лікуванні тощо), на запит роботодавця;

– обґрунтовано, що відеоспостереження за працівником на робочому місці можливе лише у випадках, необхідних для забезпечення збереження майна роботодавцю, усунення загроз здоров'ю та суспільної безпеки. Якщо працівник піддається спостереженню на робочому місці, то він має бути попередньо поінформований про причини спостереження, режим часу спостереження, використовувані методи та засоби збору інформації та отримати відповідне документування через зміни в організації виробництва і праці.

*Удосконалено:*

– науковий підхід до розуміння сутності персональних даних працівника як інформації, яка стосується загальних даних про особу працівника та/або кандидата на посаду, професійної кваліфікації працівника/кандидата на посаду, ділових, професійних якостей, а також інформація щодо спеціальних вимог, які можуть встановлюватися законодавством до працівників/кандидатів на посаду у зв'язку з характером їх роботи (приміром, заповнення декларації про доходи, проходження спеціальної перевірки тощо). Тобто персональні дані працівника мають забезпечувати ідентифікацію його/її не тільки і не стільки як людину, а насамперед як працівника;

– науковий погляд на те, що суспільні відносини, пов'язані із захистом персональних даних працівника, є окремими видами правовідносин у сфері

праці, які можуть як передувати (надання інформації в ході працевлаштування у певного роботодавця), супроводжувати (приміром, ухвалення рішення про просуванні працівника по службі), так і випливати з трудових правовідносин (приміром, розголошення комерційної таємниці), специфіка яких пов'язана з ключовими суб'єктами трудового права – працівниками та роботодавцями.

*Набули подальшого розвитку:*

– наукові позиції щодо класифікації персональних даних працівника, зокрема в аспекті їх збору, обробки та правового режиму використання на: (а) загальні «анкетні» персональні дані; (б) спеціальні персональні дані; (в) персональні дані обмеженого доступу; (г) біометричні персональні дані;

– наукова думка, що специфіка захисту персональних даних осіб, які здійснюють свою професійну діяльність на підставі трудового договору, проявляється, перш за все, в тому, що основні вимоги щодо обробки персональних даних працівника встановлюються нормами законодавства, а порядок здійснення окремих операцій з персональними даними працівника (збір, зберігання, використання, поширення) може деталізуватися у локальних правових актах.

**Практичне значення одержаних результатів** полягає в тому, що положення й висновки дисертації можуть бути використані:

– у науково-дослідницькій діяльності – з метою подальшого вивчення й розкриття порушеної проблематики, вдосконалення правового регулювання захисту персональних даних працівників;

– у навчальному процесі – при викладанні навчальної дисципліни «Трудове право», при написанні відповідних розділів підручників, навчальних посібників, курсів лекцій, а також при підготовці студентами наукових робіт;

– у правотворчості – у процесі реформування й удосконалення чинного трудового законодавства щодо правової регламентації захисту персональних даних працівників відповідно до наданих пропозицій;

– у правозастосуванні – при оперуванні наведеними висновками, рекомендаціями і пропозиціями в діяльності органів державної влади України.

**Апробація результатів дослідження.** Обговорення наукових результатів, отриманих у процесі написання дисертації, здійснювалося на публічній презентації здобувачем наукових результатів дисертації на засіданні кафедри трудового права Національного юридичного університету імені Ярослава Мудрого. Основні теоретичні положення, висновки і пропозиції автора доповідалися на міжнародних наукових і науково-практичних конференціях «Правові виклики сучасності: захист прав людини в умовах пандемії» (м. Чернівці, 22 жовт. 2021 р.), «Правове забезпечення соціальної безпеки в умовах євроінтеграційних процесів» (м. Київ, 26 листоп. 2021 р.), «Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (м. Одеса, 17 черв. 2022 р.).

**Структура дисертації.** Наукова робота складається з переліку умовних позначень, вступу, 3-х розділів, які містять 7 підрозділів, висновків, списку використаних джерел (183 найменування) і додатків. Загальний обсяг дисертації становить 216 сторінок. Обсяг основного тексту – 161 сторінка.

# РОЗДІЛ 1
# ТЕОРЕТИЧНІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ

## 1.1. Поняття і зміст персональних даних працівників

Проголошення України демократичною, соціальною, правовою державою вимагає підвищення ефективності функціонування усіх ланок суспільства. До базових засад розбудови української держави необхідно віднести й принцип гласності, що є основним чинником у забезпеченні цього конституційного положення [178, с. 27-28]. Сучасні суспільні відносини характеризуються широким використанням персональних даних під час обігу інформації (соціального, фінансового, правоохоронного, науково-технічного, управлінського характеру), товарів, послуг і капіталів. Широке використання персональних даних та виконання вимог Конституції України вимагає не тільки вільного руху інформації про особу, а також забезпечення її надійного захисту для забезпечення реалізації основних прав і свобод людини [178, с. 61].

Реалізація особами права на працю не є винятком, адже під час пошуку роботи, вступу у трудові відносини, перебігу трудових відносин тощо, особа завжди надає інформацію про себе, свою трудову діяльність, а значить ця інформація має перебувати у схоронності, тобто важливим є забезпечення захисту персональних даних працівників.

Як зазначає А. В. Авраменко, трудові правовідносини у сфері обліку та захисту персональних даних працівника виникають у зв’язку з:

– формуванням баз персональних даних працівників, осіб, які мають намір працевлаштувалися, або звільнених працівників;

– обліком персональних даних працівників з метою забезпечення реалізації ними трудової функції, зокрема обробкою даних, які визначають здатність працівника виконувати певну роботу (інформація про стан здоров’я, рівень освіти, кваліфікацію тощо), обробкою даних, які необхідні для

нарахування та виплати заробітної плати та внесків на загальнообов’язкове соціальне страхування, інших персональних даних;

– вжиттям заходів щодо забезпечення збереження та захисту персональних даних працівника і недопущення їх несанкціонованого розповсюдження та використання (використання спеціальних програмних продуктів, призначення особи, відповідальної за забезпечення захисту персональних даних працівника) тощо [76, с. 55].

Інші вчені також наголошують, що інформаційні правовідносини, що складаються між працівником та роботодавцем, є трудовими. Трудова природа правовідносини із захисту персональних даних працівника обумовлена їх суб'єктним складом, необхідністю обслуговування трудових правовідносин. Правовідносини із захисту персональних даних працівника є трудовими за змістом та інформаційними за формою. Трудовими – тому що складаються між працівником та роботодавцем у зв'язку з виникненням, зміною, реалізацією та припиненням трудових правовідносин, а інформаційними – оскільки їх здійснення можливе лише у формі певного алгоритму, обраного роботодавцем. Відтак, під трудовими інформаційними правовідносинами щодо захисту персональних даних працівника слід розуміти охоронні правовідносини, в яких одна сторона (працівник) повинна надати достовірні відомості, обов'язкові для реалізації трудових відносин, а інша сторона (роботодавець) – забезпечити цільове використання цих відомостей відповідно до норм законів, підзаконних, локальних нормативних правових актів при отриманні, зберіганні, комбінуванні, використанні та передачі зазначених відомостей третій стороні. Об'єктом правовідносини щодо захисту персональних даних працівника є відомості, віднесені до цього виду конфіденційної інформації [86, с. 19-20].

Інформаційні відносини із захисту персональних даних формуються між двома суб'єктами – роботодавцем та працівником. Право працівника на захист персональних даних тісно пов'язане з його особистістю, тому здебільшого він захищає свої інтереси самостійно, а ось на стороні роботодавця виступають уповноважені особи.

Класифікація інформації на внутрішню та зовнішню передбачає регламентацію передачі та використання інформації двома групами суб'єктів. Законодавство встановлює різний порядок доступу до персональних даних працівника всередині організації та за її межами. Перша група складається з «уповноважених роботодавцем осіб», друга – з представників «третьої сторони». В обох групах є суб'єкти, які мають право постійного доступу до персональних даних працівника, і є ті, яким це право може бути надано лише у певних випадках, спеціально передбачених у законодавстві про працю.

Правовідносини між працівником та роботодавцем із захисту персональних даних працівника є двосторонніми та зобов'язуючими. Праву працівника кореспондує обов'язок роботодавця. Праву роботодавця відповідає обов'язок працівника. У трудовому інформаційному правовідношенні із захисту персональних даних працівника на роботодавця переважно покладаються обов'язки, а працівнику надаються відповідні права. Працівник має право на повну інформацію про свої персональні дані та їх обробку роботодавцем. На вимогу працівника роботодавець зобов'язаний забезпечити доступ до персональних даних про нього. Працівники та їх представники мають бути ознайомлені під розписку з документами організації, які встановлюють порядок обробки персональних даних працівників, а також про свої права та обов'язки у цій сфері [86, с. 20-21].

Науковцями-трудовиками також висловлюється позиція, що відносини із захисту персональних даних працівника, безпосередньо пов'язані з трудовими, оскільки впливають на їх виникнення (надання інформації в ході працевлаштування у певного роботодавця), зміну (ухвалення рішення про просуванні працівника по службі) та припинення (розірвання трудового договору на підставах, пов'язаних з розголошенням персональних даних працівника роботодавцем або з наданням працівником під час укладання трудового договору свідомо неправдивої інформації). Нормативні вимоги інституту захисту персональних даних працівників спрямовані на забезпечення прав і свободи людини і громадянина роботодавцем та його представниками у процесі обробки персональних даних працівника. Ці цілі

зумовлюють охоронний характер інституту. Охоронні правові інститути мають специфіку, пов'язану із юридичною відповідальністю. Обов'язковість вимог інституту захисту персональних даних забезпечується можливістю застосування до представників роботодавця заходів дисциплінарної, адміністративної, цивільно-правової чи кримінальної відповідальності [86, с. 17].

Справедливо зазначає А. В. Авраменко, що ще з моменту прийняття документів від потенційного працівника та протягом усієї трудової діяльності особи відбувається постійне збирання, оновлення та використання певної інформації, яка становить предмет захисту адміністративного, трудового та інших галузей права [76, с. 14]. У цьому контексті, зауважимо, що серед вчених-трудовиків немає одностайної думки щодо інституційної належності відносин захисту персональних даних працівників. Деякі вчені наголошують на інструктивному характері норм захисту персональних даних працівника, що дозволяє зробити висновок про несамостійність цього інституту [85, с. 105; 75, с. 14]. Говорячи про несамостійність інституту захисту персональних даних, Г. В. Хникін зазначає, що інститут трудового договору поповнився новою групою норм, присвячених персональним даним працівника [172, с. 35].

Водночас багато дослідників вважають, що захист персональних даних працівника є самостійним інститутом. Так, у науковій юридичній літературі висловлюється думку, що суспільні відносини, які складаються щодо збору та обробки персональних даних працівників та врегульовані нормами права, є інформаційними трудовими правовідносинами, які становлять окремий інститут трудового права [80, с. 24].

Ми вважаємо, що перш за все захист персональних даних працівника є елементом трудових правовідносин, а також з метою забезпечення їх одноманітного правового режиму, захист персональних даних працівника слід розглядати як самостійний інститут трудового права. Адже суспільні відносини, пов'язані із захистом персональних даних працівника, є окремими видами правовідносин у сфері праці, які можуть як передувати (надання інформації в ході працевлаштування у певного роботодавця), супроводжувати

(приміром, ухвалення рішення про просуванні працівника по службі), так і випливати з трудових правовідносин (приміром, розголошення комерційної таємниці), специфіка яких пов'язана з ключовими суб'єктами трудового права – працівниками та роботодавцями.

Відповідно до ч. 2 та 3 ст. 24 КЗпП України [95] при укладенні трудового договору громадянин зобов'язаний подати паспорт або інший документ, що посвідчує особу, трудову книжку (у разі наявності) або відомості про трудову діяльність з реєстру застрахованих осіб Державного реєстру загальнообов’язкового державного соціального страхування, а у випадках, передбачених законодавством, – також документ про освіту (спеціальність, кваліфікацію), про стан здоров'я, відповідний військово-обліковий документ та інші документи. При укладенні трудового договору громадянин, який вперше приймається на роботу, має право подати вимогу про оформлення трудової книжки. Збір та обробка персональних даних працівника здійснюється з метою забезпечення виконання працівником його трудової функції належним чином, а також реалізації роботодавцем своїх повноважень [110, с. 239].

Хоча КЗпП України і встановлює вимоги щодо надання цих даних, однак не визначає перелік персональних даних працівників та порядок захисту персональних даних працівників. Більше того, КЗпП України не встановлює норми про захист персональних даних працівника, і, відповідно, залишається неврегульованою відповідальність за порушення порядку захисту зазначених даних [107, с. 167]. Брак законодавства, яке відповідало б сучасним міжнародним стандартам у цій сфері та рівню технологічного розвитку, не тільки призводить до незадовільного рівня захисту конституційного права на повагу до приватного життя в Україні, а й призведе до визнання на міжнародному рівні України як держави, яка не забезпечує належний рівень захисту персональних даних [109, с. 599].

Відповідно до чинного законодавства України, персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або

може бути конкретно ідентифікована (ст. 2 Закону № 2297 [137]). Правова конструкція «персональні дані» стосується лише фізичних осіб.

На жаль, ані Закон № 2297 [137], ані підзаконні акти не містять вичерпного переліку відомостей, які належать до персональних даних. Разом з цим, є орієнтовний перелік, визначений Конституційним Судом України (далі – КСУ), як інформація про особисте та сімейне життя особи (персональні дані про неї):

– національність;

– освіта;

– сімейний стан;

– релігійні переконання;

– стан здоров'я;

– матеріальний стан;

– адреса;

– дата і місце народження;

– місце проживання та перебування;

– дані про особисті майнові та немайнові відносини особи з іншими особами, зокрема членами сім'ї;

– відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування.

Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою і лише в інтересах національної безпеки, економічного добробуту та прав людини (рішення КСУ від 20.01.2012 р. № 2-рп/2012 [158]).

У науковій юридичній літературі співвідношення понять «персональні дані» та «інформація про особу» також розуміється по-різному. При цьому можна виділити принаймні два підходи. Відповідно до першого з них

«персональні дані» та «інформація про особу» розглядаються як тотожні поняття. Думається, що основним аргументом на користь такого підходу є нормативний, тобто використання в Законі України «Про інформацію» вислову «інформація про фізичну особу (персональні дані)», що тлумачиться як фактично встановлена тотожність понять «інформація про фізичну особу» та «персональні дані» [93, с. 108]. Інший аргумент є більш змістовий та полягає у сприйнятті твердження, відповідно до котрого вся інформація, здатна індивідуалізувати людину як біопсихосоціальну істоту, належить до її «персональних даних», що спричиняє визнання, що поняття «персональні дані» є практично тотожним поняттю «інформація про особу» [165, с. 86].

Представники другого підходу розуміють персональні дані вузько, розглядаючи їх особливим підвидом загального поняття «інформація про особу», вичерпний перелік яких наведено в Законі України «Про інформацію» [77, с. 902]. Наприклад, О. О. Серебряник визначає поняття інформації про фізичну особу як будь-яку інформацію (відомості та/або дані) про конкретну людину, що включає в себе її персональні дані, комунікаційні дані (метадані) та інформацію про приватне життя; розкриває расове або етнічне походження, політичні погляди, віросповідання чи філософські погляди, ставлення до конкретних подій або дій, членство у професійній спілці, місцезнаходження людини, а також дані, що стосуються її здоров'я, інтимного життя, творчості, іміджу [166, с. 10].

А. В. Кардаш стверджує, що персональні дані є елементом інформації про особу у широкому розумінні, оскільки крім персональних даних фізична особа має право формувати про себе будь-яку інформацію – як достовірну, так і недостовірну. Тому співвідносити інформацію про фізичну особу лише з персональними даними є обмеженням права людини на самостійне формування інформації про себе, яка може складатися з будь-яких відомостей/даних. Зовнішній вигляд людини є певним видом інформації про фізичну особу, але це не буде персональними даними [94, с. 90].

А ось Ю. Д. Бєлова узагальнюючи, наголошує, що кожен із зазначених підходів має раціональне зерно, й, водночас, не позбавлений певних вад. Так,

вузьке розуміння персональних даних може призвести до безпідставного обмеження захисту прав суб'єкта персональних даних, тоді як поширення правового режиму персональних даних на усю без виключення інформацію про особу може мати зворотній ефект. Вирішення цієї дилеми вбачаємо у визначенні співвідношення цих понять окремо за їх обсягом (коло відомостей, на котрі поширюється дане поняття) та змістом (сукупність існуючих ознак таких відомостей, відображених у понятті). За обсягом ці поняття є фактично тотожні, оскільки будь-яка інформація про особу може її ідентифікувати. У той же час, за змістом ці поняття потрібно розмежовувати. В якості розмежувальної ознаки пропонуємо використовувати факт обробки відповідних відомостей. Тобто, інформація про особу набуває правового режиму персональних даних внаслідок того, що стає предметом обробки [79, с. 40].

На думку М. В. Різаки, Закон України № 2297 [137] у поняття «персональні дані» вкладає досить широкий зміст, що підтверджується відкритістю переліку відомостей, віднесених до числа персональних даних. Виходячи із самої природи персональних даних, повністю їх перерахувати досить складно. Це й зумовило підхід законодавця, згідно з яким суб'єкт має право частково самостійно формувати свій «інформаційний портрет», вирішуючи, які з характеристик, що його ідентифікують, слід віднести до числа персональних даних, а які ні [154, с. 128].

Відзначимо, що у науці виділяють об'єктивну та суб'єктивну можливості ідентифікації суб'єкта даних. У першому випадку ідентифікація проводиться виключно на основі уже наявної інформації, яка є предметом розгляду. Суб'єктивно можлива ідентифікація, що додатково передбачає аналіз й іншої інформації, одержання якої потребує «розумних зусиль», або до якої може одержати доступ особа, відповідальна за обробку даних. Враховуючи інтереси особи, у вітчизняному законодавстві варто було би надати перевагу суб'єктивно можливій ідентифікації, так як це забезпечить більш надійний ступінь захисту прав фізичної особи, особливо у стосунках із професійними організаціями, котрі можуть мати значні ресурси для пошуку і

аналізу інформації [88, с. 6]. Ознака ідентифікації є ключовою в понятті «персональних даних»; саме вона є визначальною при поширенні на відомості правового режиму персональних даних. Натомість, виокремлюють так зване знеособлення персональних даних, вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу. Це, наприклад, може бути потрібно у тих випадках, коли законні цілі, відповідно до котрих дані збиралися або надалі оброблялися, відпали. При цьому слід пам'ятати, що для знеособлення персональних даних можливість прямо чи опосередковано ідентифікувати фізичну особу повинна встановлюватися в кожному окремому випадку [79, с. 46-47].

Наголосимо, що зміст інформації про фізичну особу (персональні дані) залежить від характеру правовідносин, в яких вони отримують своє наповнення. Це зумовлено специфікою відповідної правової регламентації цих відносин. Власне інформація про фізичну особу (персональні дані) не є універсальним поняттям, що має тотожній зміст у сфері приватного чи публічного права [87]. Виходячи із цієї позиції, зміст поняття «персональні дані» різниться в залежності від виду правовідносин, в яких відбувається їх захист. Відповідно, поняття «персональні дані працівника» є спеціальним по відношенню до більш загального поняття – «персональні дані».

У науковій юридичній літературі дослідниками запропоновано різноманітні варіанти класифікації персональних даних:

1) за ступенем пов'язаності з особою персональні дані поділяють на постійні (колір очей) та змінювані (адреса проживання, місце роботи) [177, с. 153-162];

2) за співвідношенням із метою використання – на повні, неповні та надмірні (виходячи з тлумачення ст. 6 Закону «Про захист персональних даних»);

3) залежно від того, якими органами чуття сприймаються персональні дані – на звукові і зорові (включаючи символьні (зокрема текст) та образні (зокрема, фото)); ті, що сприймаються безпосередньо органами чуття

(містяться в документах, портретах), і ті, для обробки яких потрібна спеціальна апаратура (зчитувач скану сітківки ока, комп'ютер тощо) [88, с. 8];

4) за особливостями правового регулювання: загальні персональні дані – прізвище, ім'я та по батькові, дата народження, а також інші персональні дані, які за згодою суб'єкта цих даних розміщені в загальнодоступних базах персональних даних та які на момент їх обігу та/або обробки не були вилучені або знищені з цих баз; вразливі персональні дані – відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, звинувачення у скоєнні злочину або засудження до кримінального покарання, а також дані, що стосуються здоров'я чи статевого життя; спеціальні персональні дані – персональні дані, що не входять до вразливих чи загальних персональних даних, межі обігу яких визначаються суб'єктом цих даних [153, с. 94].

Персональні дані можуть класифікуватися й за іншими критеріями: за предметом (біографічні, фінансові, біометричні тощо), ступенем потенційної шкідливості неконтрольованого обігу (звичайні, вразливі), здатністю до ідентифікації (прямо та опосередковано ідентифікуючі), формою фіксації (символи, образи, сигнали), співвідносністю з метою використання (повні, неповні, надмірні), адекватністю відображення дійсності (достовірні, недостовірні), способом сприйняття людиною (безпосередньо або за допомогою технічних засобів) тощо [88, с. 9].

На думку деяких вчених, до мінімального обсягу відомостей, які дозволяють ідентифікувати особу, можна віднести інформацію про прізвище, ім'я та по батькові особи разом з датою її народження або домашньою, поштовою чи електронною адресою, або номером телефону, або індивідуальним податковим номером [113, с. 61]. Уявляється можливим до загальних персональних даних працівників включити інформацію про його паспортні дані, інформацію з картки платника податків, про кваліфікацію, освіту, трудовий стаж та досвід роботи на відповідній посаді [76, с. 19-20].

Р. В. Куценко, що структуру персональних даних працівника складають такі групи відомостей про фізичну особу:

1) відомості про фізичну особу, які подаються для вирішення питання про прийняття на роботу (до укладення трудового договору). Обсяг таких відомостей залежить від вакантної посади і може включати інформацію щодо прізвища, ім’я, по батькові особи, адреси її проживання та інші паспортних даних, досвіду роботи, рівня кваліфікації та освіти тощо;

2) загальні відомості про фізичну особу, які подаються при укладені трудового договору незалежно від трудової функції та посади, яку обіймає працівник: паспортні дані, інформація, що міститься у трудовій книжці, картка платника податків (за наявності) та ін.;

3) особливі відомості, що подаються для формування персональних даних працівників окремих категорій: інформація про стан здоров’я, наявність водійських прав тощо;

4) інформація, що накопичується в процесі роботи працівника: відомості про розмір оплати праці, заохочення та дисциплінарні стягнення, характеристика тощо;

5) відомості, що зберігаються після звільнення працівника (після розірвання трудового договору): всі відомості, які містяться в особовій справі працівника, включаючи ті, що були подані до укладення трудового договору та виникли в процесі виконання трудової функції [100, с. 245].

А. М. Чернобай переконаний, що поняття персональних даних працівника вужче поняття персональних даних про особу, оскільки йдеться не про всі відомості (факти, події, обставини життя фізичної особи), а тільки про такі обставини, що можуть характеризувати фізичну особу як працівника. Персональні дані працівника потрібно розглядати як будь-яку інформацію, яка стосується конкретного працівника та необхідна роботодавцю у зв'язку з використанням праці цього працівника на підставі трудового договору. Це може бути тільки така інформація, яка необхідна роботодавцю у зв'язку з трудовими правовідносинами.

Персональні дані працівника належать до категорії документованої інформації, тобто інформації, зафіксованої на матеріальному носію з реквізитами, що дозволяють її ідентифікувати. Крім того, персональні дані

працівника, занесені до особових справ і документів обліку, є персоніфікованими, такими, що носять конфіденційний характер. У деяких випадках персональні дані працівника можуть становити державну таємницю.

Залежно від наявності суб'єктивного фактору персональні дані працівника можна поділити на два види: 1) фактичні дані, які не підлягають суб'єктивній оцінці (про набуту після закінчення навчального закладу спеціальність, службу у Збройних Силах України» інших військових формуваннях тощо); 2) персональні дані оціночного характеру, які можуть міститися у виробничій (службовій) характеристиці, висновку атестаційної комісії тощо.

Залежно від часу подання або формування відомості, що складають персональні дані працівника, поділяються на: 1) відомості, що подаються працівником при прийнятті на роботу і містяться у поданих працівником документах (відомості у паспорті або іншому документі, що засвідчує особу працівника; відомості у трудовій книжці; відомості про освіту, кваліфікацію; відомості, які містяться в документі медичного огляду працівника (зокрема, медичній книжці) та ін.); 2) відомості, які формуються, отримуються та використовуються роботодавцем у період трудової діяльності працівника (відомості, які містяться в особовій справі працівника, у наказах, розпорядженнях, характеристиках, атестаційних справах та ін.); 3) відомості про працівника, які зберігаються у роботодавця після припинення з ним трудових правовідносин (усі персональні дані працівника, які є в архіві організації) [175, с. 9-10].

А ось Р. І. Чанишев вважає, що персональні дані працівника потрібно розуміти як будь-яку інформацію, яка стосується конкретного працівника та необхідна роботодавцю у зв’язку з використанням праці цього працівника на умовах трудового договору. Це може бути тільки така інформація, яка необхідна роботодавцю у зв’язку з трудовими правовідносинами [174, с. 75].

Розвиваючи думку науковця, можемо стверджувати, що всю сукупність персональних даних можна поділити на дві групи: 1) персональні дані, необхідні для існування трудових правовідносин, визначаються КЗпП України

та іншими нормативно-правовими актами; 2) всі інші персональні дані. Зрозуміло, що роботодавець має отримати лише ту кількість персональних даних, які є необхідними для оформлення правовідносин із працівником, все інше – особисте життя людини, яке перебуває поза межами впливу роботодавця. Персональні дані працівника, які містяться в паспорті або документі, що посвідчує особу, в трудовій книжці, документі про освіту (спеціальність, кваліфікацію), документі про стан здоров'я та інших документах, які він подав при укладенні трудового договору, обробляються володільцем бази персональних даних на підставі ст. 24 КЗпП України виключно для здійснення повноважень володільця бази персональних даних у сфері правовідносин, які виникли в нього з працівником на підставі трудового договору (контракту). Таким чином, інформація про найманих працівників є базою персональних даних, оскільки особові справи, трудові книжки, копії паспортів, документів про освіту зберігаються та обробляються роботодавцем [147]. У зв'язку з цим до структури персональних даних працівника мають належати лише ті з них, які є достатніми для укладення трудового договору. Залежно від особливостей трудової функції доцільно нормативно визначити загальну структуру персональних даних працівників та структуру, характерну для окремих спеціальностей.

Як слушно зазначає Т. І. Обуховська, згідно із законодавством більшості європейських держав персональні дані розділяються за критерієм «чутливості» на дані загального характеру (прізвище, ім'я, по батькові, дата і місце народження, громадянство, місце проживання) і «чутливі» (вразливі) персональні дані (дані про стан здоров'я (історія хвороби, діагнози), етнічна належність, ставлення до релігії, ідентифікаційні коди чи номери, відбитки пальців, записи голосу, фотографії, кредитна історія, дані про судимість тощо). Для «чутливих» персональних даних передбачений більш високий ступінь захисту. Так, забороняється збирання, зберігання, використання та передача без згоди суб'єкта саме «чутливих» даних, а не всіх персональних даних [111, с. 100].

Чутливі персональні дані — це відомості, обробка яких становить особливий ризик для прав і свобод людей. Володільці, які обробляють чутливі дані, повідомляють про це Уповноваженого Верховної Ради України з прав людини (омбудсмена). До 2014 року діяла процедура реєстрації баз персональних даних у Реєстрі, який вела Держслужба з питань захисту персональних даних. Відтак, процедуру скасували, а їй на заміну ввели іншу — повідомлення омбудсмена. Порядок повідомлення визначено наказом омбудсмена від 08.01.2014 р. № 1/02-14 [128].

Так, до персональних даних, обробка яких становить особливий ризик для прав і свобод людей (тобто чутливі персональні дані), належать:

– відомості про расове, етнічне та національне походження;

– відомості про політичні, релігійні або світоглядні переконання;

– відомості про членство в політичних партіях та (або) організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;

– відомості про стан здоров’я;

– відомості про статеве життя;

– біометричні дані;

– генетичні дані;

– відомості про притягнення до адміністративної чи кримінальної відповідальності;

– відомості про застосування щодо особи заходів в рамках досудового розслідування; вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність» від 18.02.1992 р. № 2135-XII [144];

– відомості про вчинення щодо особи насильства;

– дані про місцеперебування та (або) шляхи пересування особи (п. 1.2 Порядку повідомлення [128]).

Якщо підприємство обробляє чутливі персональні дані, то подає омбудсмену заяву про обробку персональних даних, яка становить особливий

ризик для прав і свобод суб'єктів персональних даних (Додаток 1 до Порядку повідомлення [128]).

Цікавою є позиція омбудсмена щодо інформації про заробітну плату та інші виплати працівнику державного органу або органу місцевого самоврядування, де висловлено позицію, що ця інформація є інформацією про фізичну особу. Так, публічний характер як самих органів-суб'єктів владних повноважень, так і їх посадових осіб вимагає оприлюднення певної інформації для формування громадської думки про довіру до влади та підтримку її авторитету у суспільстві. Розпорядження бюджетними коштами включає здійснення витрат з державного чи місцевого бюджету. Заробітна плата та інші виплати (премії, матеріальна допомога тощо) посадовим та службовим особам є витратами з бюджету. Відповідно до ч. 5 ст. 6 Закону України «Про доступ до публічної інформації» [125] визначено, що не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. Це підтверджується положенням ст. 5 Закону України «Про захист персональних даних» [137], у якій йдеться про те, що не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень, а також «не належить до інформації з обмеженим доступом інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених ст. 6 Закону України «Про доступ до публічної інформації» [125].

Отже, інформація про заробітну плату, премії, матеріальну допомогу, будь-які інші виплати з державного чи місцевого бюджету працівнику державного органу або органу місцевого самоврядування не є конфіденційною, не може бути обмежена в доступі та підлягає наданню на запит [112].

Ми погоджуємося із такою позицією, однак на практиці повсякчас виникають проблеми щодо захисту даних про заробітну плату працівників. Проілюструємо судовою справою. Так, позивачка звернулась до суду з позовом до Комунального підприємства «Будинок книги» Чернігівської міської ради та просила визнати незаконним та скасувати наказ від 22.10.2019 р. про притягнення її до дисциплінарної відповідальності. Відповідно до наказу директора від 22.10.2019 р. їй була оголошена догана за порушення трудової дисципліни, а саме: за не забезпечення захисту від незаконного доступу та розповсюдження персональних даних працівників без їх згоди.

27.11.2019 р. до суду від відповідача надійшов відзив на позовну заяву, згідно з яким відповідач просить у задоволенні позовних вимог відмовити в повному обсязі. Адже згідно з наказом від 25.12.2013 р. головний бухгалтер (позивачка) отримала доступ до персональних даних працівників виключно для використання зі службовою метою, проте позивачка використала персональні дані працівників підприємства, а саме – відомості про отримані суми винагород (премії) протягом минулих років, у особистих цілях без згоди працівників.

Відповідач стверджував, що догану від 22.10.2019 р. було винесено головному бухгалтеру (позивачці), оскільки вона поширила персональні дані щодо працівників підприємства, про що стало відомо 25.09.2019 р. на загальних зборах (що і є днем виявлення проступку). Керівник підприємства повідомила на загальних зборах працівникам про надання позивачкою Новозаводському районному суду м. Чернігова, а також міському голові наказів про преміювання працівників. Однак вказані документи мають персональні дані інформацію про майновий стан осіб, яка охороняється законом, і не повинна була розголошуватись позивачем без згоди, останній було оголошено догану.

Підставою для винесення оскаржуваного наказу були скарги працівників підприємства щодо розголошення головним бухгалтером (позивачкою) КП «Будинок книги» персональних даних, зокрема сум нарахованих та отриманих працівниками премій протягом минулих періодів. Ці дані без дозволу працівників були розголошені під час подачі скарги до Чернігівського міського голови від 23.05.2019 р. та заяви до Новозаводського районного суду м.

Чернігова від 29.08.2019 р., до яких були приєднані відповідні накази по підприємству.

Суд, дослідивши матеріали справи та, вислухавши доводи сторін, дійшов висновку, що враховуючи, те що КП «Будинок книги» Чернігівської міської ради є комунальним підприємством, яке підпорядковане Чернігівській міській раді, а позивачка (головний бухгалтер) звернулась до голови Чернігівської міської ради зі скаргою, до якої надала копії наказів, але ці накази не містять державної чи службової таємниці, а також інформації з обмеженим доступом в розумінні ч. 3 ст. 5 Закону України «Про захист персональних даних», а тому суд дійшов висновку про відсутність порушень з боку головного бухгалтера КП «Будинок книги» Чернігівської міської ради.

Крім того, суд зазначив, що стороною відповідача стверджувалося, що днем виявлення вказаного у наказі порушення трудової дисципліни, слід вважати 25.09.2019 р. – день проведення загальних зборів трудового колективу підприємства. Однак суд не погодився з такими твердженнями з огляду на наступне.

Як вбачається зі змісту рішення Новозаводського районного суду м. Чернігова від 21.10.2019 р., залишеним без змін постановою Чернігівського апеляційного суду від 27.12.2019 р., у цивільній справі № 751/6123/19, у якій брали участь ті самі сторони, в судовому засіданні представник відповідача КП «Будинок книги» пояснювала: «директор підприємства дізналась про подану головним бухгалтером скаргу на початку червня 2019 року, точну дату не знає. Скарга датована 24.05.2019 р. та отримана 25.05.2019 р. До скарги позивачка додала копії наказів, які отримані нею незаконним шляхом, оскільки з заявою про видачу копій не зверталась…».

Також вищевказаним рішенням суду встановлено, що «26.06.2019 р. КП «Будинок книги» на ім`я позивачки (головного бухгалтера) було надіслано повідомлення (вимога), згідно з якою її просять у строк до 17.00 26.06.2019 р. надати письмове пояснення щодо того, на підставі – яких норм внутрішніх чи інших актів, посадової інструкції або інших документів, нею було завірено копії наказів підприємства про преміювання.

Із вищевикладеного суд вбачав, що керівник КП «Будинок книги» про звернення позивачки до голови Чернігівського міського голови зі скаргою, до якої були долучені накази про преміювання працівників КП «Будинок книги» був обізнаний лише в червні–липні 2019 року.

Таким чином, наказ директора КП «Будинок книги» Чернігівської міської ради від 22 жовтня 2019 року про оголошення догани позивачці винесено з порушенням місячного строку, встановленого ст. 148 КЗпП України [160].

Варто зауважити, що свого часу Державна служба України з питань захисту персональних даних (наразі ліквідована) у своєму листі від 02.04.2012 р. №10/1106-12 «Щодо персональний даних» [179] рекомендувала вважати персональними даними всю інформацію про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, у тому числі й інформацію у візитівці, адресній книзі електронної пошти, а також список контактів у мобільному телефоні. Вважаємо, що інформація у цих видах інформаційних джерел не має бути об’єктом захисту персональних даних, а особливо в аспекті трудових правовідносин, адже особа сама ініціює виготовлення візитівок як раз з тією метою, щоб популяризувати або себе, або послуги, які надає.

У науковій юридичній літературі персональні дані визначаються як відомості або сукупність відомостей, які безпосередньо чи опосередковано стосуються фізичної особи, незалежно від її громадянства, постійного місця проживання чи іншого правового зв’язку з державою, що є їх носієм, та дозволяють «прямо» або «опосередковано» її ідентифікувати за умови, що такі відомості було оброблено шляхом збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення знеособлення, знищення, у тому числі – із використанням інформаційних (автоматизованих) систем [79, с. 52]. Інші науковці стверджують, що персональні дані працівника – це система відомостей про особу, з якою укладається трудовий договір, що формується, накопичується, зберігається, використовується тощо роботодавцем у порядку, визначеному законодавством, з метою ідентифікації особи працівника, прийняття рішень, пов’язаних з виконанням його трудової функції, зміною або розірванням трудового договору

[76, с. 66-67]. Під персональними даними працівника також розуміються встановлені законом або на підставі закону відомості про факти, події та обставини життя конкретного працівника, які він/вона пред'являє роботодавцю, які збираються про нього/неї, з метою сприяння працівнику у працевлаштуванні, навчанні, просуванні по службі, забезпечення особистої безпеки, продуктивного використання робочого часу, якісного виконання роботи та забезпечення збереження майна організації [86, с. 6-7].

Вважаємо, що персональні дані працівника – це інформація, яка стосується загальних даних про особу працівника та/або кандидата на посаду, професійної кваліфікації працівника/кандидата на посаду, ділових, професійних якостей, а також інформація щодо спеціальних вимог, які можуть встановлюватися законодавством до працівників/кандидатів на посаду у зв'язку з характером їх роботи (приміром, заповнення декларації про доходи, проходження спеціальної перевірки тощо). Тобто персональні дані працівника мають забезпечувати ідентифікацію його/її не тільки і не стільки як людину, а насамперед як працівника. Це означає, що персональні дані працівника та претендента на посаду – це, в першу чергу, інформація, що стосується професійної кваліфікації, ділових, професійних якостей та відповідності працівника та претендента на посаду вимогам, які можуть бути до нього пред'явлені у зв'язку з характером роботи.

Відповідно до цього, на нашу думку, варто провадити класифікацію персональних даних працівника, в аспекті їх збору, обробки та правового режиму використання:

– загальні «анкетні» персональні дані (відомості про прізвище, ім’я, по батькові, дата та місце народження, паспортні дані, відомості про освіту, про професійні навички, відомості про «історію» трудової діяльності тощо);

– спеціальні персональні дані: расова, національна приналежність, політичні погляди, релігійні чи філософські переконання, стан здоров'я, приватне життя. Збір та обробка цих персональних даних має бути заборонена для роботодавця;

– персональні дані обмеженого доступу, до яких слід віднести відомості про усиновлення, судимість, участі у кримінальному судочинстві як підозрюваного, наданої чи прийнятої фінансової допомоги, чи послуг, декларація про доходи, результати спеціальної перевірки тощо;

– біометричні персональні дані – відомості, що містять характеристики фізіологічних та біологічних особливостей людини, що дають можливість встановлення її особистості. Ці дані є «чутливими даними» і мають особливий правовий режим захисту. Для їх обробки роботодавцем потрібне спеціальне погодження Уповноваженим ВРУ.

## 1.2. Основні концептуальні підходи до дослідження механізмів забезпечення захисту персональних даних працівників

Збирання, зберігання та обробка персональних даних особи у сфері трудових правовідносин починається ще на стадії підготовки до укладення трудового договору, коли суб'єкт персональних даних не отримав статус працівника. На цьому етапі обіг інформації про особу здійснюється з метою працевлаштування такої особи, проходження нею конкурсів та відборів на певну посаду. Подальший збір та обробка персональних даних працівника обумовлений завданням забезпечення виконання трудової функції, захисту прав та інтересів працівника та роботодавця [76, с. 72].

Поняття захисту персональних даних є доволі широким та зазвичай включає два ключових елемента. По-перше, це зобов'язання володільця вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних (ст. 24 ЗУ «Про захист персональних даних» [136]). По-друге, це зобов'язання кожного працівника володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, так зване зобов'язання конфіденційності (ст. 10 Закону № 2297 [136]).

Володілець персональних даних самостійно повинен визначати, яких заходів слід вживати з метою забезпечення захисту персональних даних. При цьому слід враховувати вимоги законодавства у сфері захисту персональних даних та інформаційної безпеки. Вказана вимога стосується усіх володільців. Перелік обов'язкових заходів захисту, які повинні вживатися всіма володільцями, визначено Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого від 08.01.2014 р. № 1/02-14 [128]. Ці вимоги носять загальний характер і є мінімальними вимогами у сфері захисту персональних даних, а шляхи їх практичної імплементації вирішуються в індивідуальному порядку кожним окремим володільцем.

Основними елементами механізму правового регулювання захисту персональних даних є: інформаційне середовище суб'єктів владних повноважень, завдання, принципи, суб'єкти, об'єкти, засоби регулювання використання персональних даних суб'єктами владних повноважень та гарантії забезпечення законності у цій сфері.

Можна виокремити такі принципи захисту персональних даних працівника [168, с. 72]:

– принцип добровільності надання персональних даних особою під час влаштування на роботу;

– принцип достовірності та повноти інформації, що складає персональні дані працівника;

– принцип адекватності, достатності та ненадмірності збору і обробки персональних даних працівник;

– принцип відповідальності роботодавця за стан збереження та забезпечення захисту персональних даних працівника;

– принцип безперервності забезпечення захисту персональних даних працівника;

– принцип використання персональних даних працівника роботодавцем виключно з метою забезпечення виконання працівником трудової функції та виконання роботодавцем своїх повноважень;

– принцип відкритості та прозорості використання роботодавцем персональних даних працівника;

– принцип чіткості визначення мети збору та використання персональних даних працівника;

– принцип виключності випадків обмеження прав працівника при обробці його персональних даних.

Розглянуті вище принципи захисту персональних даних працівника складають фундаментальні засади, на яких функціонує механізм захисту персональних даних [78, с. 20-32].

Механізм правового регулювання захисту персональних даних є системою правових, організаційних, технічних засобів забезпечення законності, ефективності та доцільності використання персональних даних суб'єктами владних повноважень із дотриманням балансу суспільного інтересу та права на приватність [178, с. 85].

Механізм захисту персональних даних працівників – це система елементів та засобів, що забезпечують цілісність, недоторканність та достовірність особистих відомостей про працівника, а також передбачену законодавством процедуру збирання, використання, оновлення, обробки, зберігання та знищення такої інформації, визначають підстави та процедуру притягнення до відповідальності правопорушників та встановлюють порядок відшкодування заподіяної ними шкоди [76, с. 152].

Говорячи про суб'єктний склад трудових правовідносин, необхідно вказати на особливий статус, який набувають суб'єкти трудових правовідносин у процесі захисту персональних даних працівника. Зокрема, працівник як обов'язковий суб'єкт трудових правовідносин є суб'єктом персональних даних у розумінні Закону України № 2297 [137]. При цьому роботодавець у таких правовідносинах має статус володільця персональних даних, оскільки визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом. Окрім працівника та роботодавця, як суб'єктів та володільців персональних даних працівника, учасниками трудових

правовідносин у досліджуваній сфері можуть виступати треті особи – одержувачі та розпорядники персональних даних.

Суб'єктний склад трудових правовідносин у даній сфері може мати такий вигляд:

– суб'єктом персональних даних витупає працівник, кандидат на певну посаду під час проходження кадрового добору, особа, звільнена з певної посади протягом періоду зберігання її персональних даних у роботодавця;

– володільцем персональних даних працівника є роботодавець, підприємство, установа, організація, фізична особа-суб'єкт підприємницької діяльності, з якими особа має намір укласти трудовий договір (пройти конкурсний добір) та подає документи або з якими трудовий договір розірвано;

– одержувачем персональних даних, у тому числі третьою особою, може виступати конкурсна комісія, кадрові служби, служби зайнятості, розробники сайтів тощо, тобто суб'єкти, які в інтересах роботодавця здійснюють збір, оброблення та зберігання інформації про потенційного працівника;

– розпорядник персональних даних працівника – особи, яким роботодавець доручає обробку персональних даних працівника. До таких, наприклад, можна віднести бухгалтера, який не є працівником підприємства, банківські установи, архівні установи тощо [76, с. 54].

С. Л. Гнатюк зазначає, що основи ідеології захисту персональних даних у правовій практиці сучасних демократичних держав можна звести до таких двох положень: 1) пріоритетним є право особи розпоряджатися своїми персональними даними; їх використання без дозволу володільця карається згідно із законодавством; 2) для будь-кого, хто здійснює користування персональними даними фізичних осіб з їх дозволу, встановлено відповідальність у разі умисного розголошування цих даних третім особам (якщо тільки фізична особа не дала дозвіл на таке розголошування) [84, с. 5-6].

Захист персональних даних працівника – це сукупність організаційно-правових, інженерно-технічних, криптографічних та інших заходів, які вживаються власником інформації з обмеженим доступом або іншими особами за його замовленням, з метою запобігання заподіянню шкоди інтересам власника

інформації та особи, якої вона стосується, її неконтрольованому поширенню [176, с. 124].

Знищення персональних даних працівника – це дія, що полягає у виключенні інформації про працівника із баз даних роботодавця та/або третіх осіб, у тому числі шляхом видалення або інших дій, внаслідок яких інформація, що складає персональні дані працівника, припиняє існувати [76, с. 107]. На практиці часто виникає запитання – чи можна знищити персональні дані працівника на його вимогу? Вважаємо, що не можна, оскільки роботодавець порушить законодавство, якщо знищить на вимогу працівника документи, для яких встановлено строк зберігання.

Така ситуація виникає із працівниками, які звільняються, і звертаються до кадрової служби з вимогою знищити після їх звільнення всі персональні дані, приміром особову справу чи картку П-2 тощо. Працівники посилаються на те, що таке право передбачено законом. Право, дійсно, є, але на сферу трудових відносин воно не поширюється. Так, працівник як суб'єкт персональних даних має право пред'являти вмотивовану вимогу щодо знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними (п. 6 ст. 8 Закону № 2297 [137]).

Відповідно до чинного законодавства персональні дані знищують, якщо:

– їх зібрали з порушенням вимог Закону № 2297 [137];

– припинено правовідносини між суб'єктом персональних даних та володільцем чи розпорядником персональних даних, якщо інше не передбачено законом (ст. 15 Закону № 2297 [137]).

Знищувати персональні дані на вимогу працівника у зв'язку з припиненням правовідносин між працівником і роботодавцем, неправомірно, адже ст. 15 Закону № 2297 [137] визначає ще одну вимогу: персональні дані підлягають знищенню в разі закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом.

Норми національного законодавства не закріплюють належного механізму реалізації права особи на звернення до володільця чи персональних

даних з вимогою щодо їх знищення, оскільки передбачає лише дві умови, за яких суб'єкт персональних даних може звернутися з відповідною вимогою. Вважаємо, що такий підхід не цілком узгоджується з європейськими нормами та потребує удосконалення, зокрема, шляхом розширення переліку умов, за наявності яких суб'єкт персональних даних може звернутися до володільця з вимогою про їх знищення. До таких умов доцільно додатково віднести, наприклад, вичерпання мети, з якою була надана згода суб'єкта персональних даних на їх збирання та обробку тощо [76, с. 108].

На законодавчому рівні строки зберігання організаційно-розпорядчих, бухгалтерських, первинних облікових документів, особових справ визначає Перелік типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів від 12.04.2012 р. № 578/5 (далі – Перелік) [130]. Визначені в Переліку строки зберігання документів, є мінімальними, їх не можна скорочувати.

Відтак, роботодавець не має права знищувати документи з персональними даними працівника (особову картку П-2 чи документи особової справи), адже за законом їх треба зберігати 75 років (п. 1.7 Переліку). У працівника як суб'єкта персональних даних є право вмотивованої вимоги знищити персональні дані. Однак, право виникає лише тоді, коли дані обробляються незаконно чи є недостовірними.

Закон № 2297 [137] уводить спеціальні назви для всіх учасників у сфері захисту персональних даних (ст. 4 Закону № 2297 [137]).

**Суб'єкти відносин, пов'язаних із персональними даними [182]**

| Суб'єкт | Хто це | Приклад |
|---|---|---|
| Суб'єкт персональних даних | Фізична особа, персональні дані якої обробляються | Суб'єктом персональних даних є працівник чи особа, яка виконує роботи за цивільно-правовим договором |

| | | |
|---|---|---|
| Володілець персональних даних | Фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки (якщо інше не визначено законом) | З метою реалізації трудових відносин будь-яке підприємство збирає, опрацьовує, зберігає відомості про своїх працівників, отже, з погляду Закону № 2297 [137] є володільцем персональних даних працівників |
| Розпорядник персональних даних | Фізична чи юридична особа, якій володільцем або законом надано право обробляти ці дані від імені володільця. Розпорядник може обробляти персональні дані лише з метою і в обсязі, визначених у договорі з володільцем.<br><br>Розпорядники є не завжди | Немає відділу кадрів, а кадрове діловодство веде стороння консалтингова фірма. Ця фірма вважається розпорядником персональних даних |
| Третя особа | Будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника та Уповноваженого ВРУ з прав людини, якій володілець чи розпорядник передають персональні дані | Органи ПФУ, військові комісаріати, органи прокуратури.<br><br>Підприємство отримало запит про надання певних персональних даних працівника від адвоката, органу прокуратури, суду, банку, поліції, ДМС. Усі ці органи є третіми особами |
| Уповноважений ВРУ з прав людини | Орган, що контролює та розробляє нормативні акти із захисту персональних даних | |

Таким чином, специфіка захисту персональних даних осіб, які здійснюють свою професійну діяльність на підставі трудового договору, проявляється, перш за все, в тому, що основні вимоги щодо обробки персональних даних працівника встановлюються нормами законодавства, а порядок здійснення окремих операцій з персональними даними працівника (збір, зберігання, використання, поширення) може деталізуватися у локальних

правових актах. Обов'язок не розголошувати персональні дані також може бути передбачений законами та підзаконними актами для окремих категорій осіб, наприклад, для державних службовців.

Можна виокремити чотири кроки, щоб захистити персональні дані працівника на підприємстві:

1. Визначити технічні та організаційні заходи, які треба вжити.

2. Призначити відповідального за обробку і захист персональних даних. Якщо роботодавець – орган влади, ОМС чи підприємство, що обробляє чутливі персональні дані, призначайте відповідального обов’язкового. В інших випадках – за рішенням керівника підприємства.

3. Розробити Положення про порядок обробки та захисту персональних даних.

4. Отримати зобов’язання про нерозголошення персональних даних від працівників, які стикаються під час роботи з персональними даними інших осіб. Зареєструвати отримані зобов’язання в Журналі реєстрації зобов’язань про нерозголошення персональних даних.

Відповідальний (особа чи цілий підрозділ) має бути в органі влади чи місцевого самоврядування, а також на підприємстві, що обробляє чутливі персональні дані і підпадає під обов’язок повідомляти про обробку Уповноваженого ВР з прав людини (ст. 24 Закону № 2297 [137]). Таке підприємство повідомляє Уповноваженого ВР з прав людини не лише про обробку чутливих даних, а й про те, кого призначили відповідальним.

Підприємства, на які не поширюється обов’язок із повідомлення Уповноваженого ВР з прав людини, самостійно визначають, чи призначати відповідального (п. 3.22 Типового порядку обробки ПД [128]).

Головна функція відповідального за захист персональних даних — організація роботи. Працівників, які безпосередньо працюватимуть із персональними даними (відділ кадрів, бухгалтерія, реєстратура або медичний персонал закладу охорони здоров’я тощо), може бути багато. Однак, має бути особа, що координуватиме і контролюватиме дотримання процедур роботи з персональними даними.

Відповідальний:

| | |
|---|---|
| – інформує та консультує володільця або розпорядника персональних даних із питань додержання законодавства про захист персональних даних | п. 3.17 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого ВР з прав людини від 08.01.2014 № 1/02-14 [128] |
| – взаємодіє з Уповноваженим ВР з прав людини та визначеними ним посадовими особами його Секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних | |
| – стежить за дотриманням прав суб'єктів персональних даних | п. 3.18 Типового порядку обробки ПД [128] |
| – аналізує загрози безпеці персональних даних | |
| – виявляє та фіксує порушення і повідомляє про них керівництво | п. 3.20 Типового порядку обробки ПД [128] |

Права й обов'язки відповідального мають бути чітко визначені в Положенні про порядок обробки і захисту персональних даних. Навіть якщо підприємству не потрібно повідомляти Уповноваженого ВР з прав людини про обробку персональних даних, радимо визначати відповідальну особу за роботу із захисту персональних даних. Якщо за певну ділянку ніхто конкретно не відповідає, то і спитати нема з кого.

Відповідальний (особа чи підрозділ) має бути в органі влади чи місцевого самоврядування, а також на підприємстві, що обробляє чутливі персональні дані і підпадає під обов'язок повідомляти про таку обробку Уповноваженого ВР з прав людини (ст. 24 Закону № 2297-VI [137]). Підприємства, на які не поширюється обов'язок повідомляти Уповноваженого ВР з прав людини, самостійно визначають, чи призначати відповідального (п. 3.22 Типового порядку обробки ПД [128]). Кого саме призначити відповідальним за обробку персональних даних – не відповідають ані Закон № 2297-VI [137], ані Типовий порядок обробки ПД [128]. Орієнтуватися варто на специфіку підприємства і на його фахівців. Відповідальний повинен мати навички аналітичної роботи і

роботи із нормативно-правовими актами, розвинені управлінські компетенції. Це випливає з Типового порядку обробки ПД [128]. Як правило, такими компетенціями володіють керівники підприємств, їхні заступники і керівники структурних підрозділів.

Працівник, якого призначили відповідальним за ЗПД, не несе абсолютної та безумовної відповідальності, якщо Уповноважений ВР з прав людини виявить порушення законодавства про ЗПД.

Обов'язок відповідального – організувати процес як належить. Особа нестиме відповідальність тільки, якщо халатно виконуватиме свої посадові обов'язки. До відповідальності притягнуть того, хто дійсно вчинив порушення. Хто винен чи причетний до порушення, визначають під час перевірки.

Важливо визначити – чи є відповідальність за відсутність Положення про захист персональних даних? Наголосимо, що роботодавця не оштрафують за те, що на підприємстві немає Положення про порядок обробки і захисту персональних даних працівників. Утім, відсутність унормованих процедур може спричинити порушення, за які передбачено адміністративну відповідальність (ст. 188-39, 188-40 КУпАП [96]).

Володільці, розпорядники персональних даних і треті особи зобов'язані забезпечити захист цих даних від випадкової втрати або знищення, від незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних (ч. 1 ст. 24 Закону № 2297 [137]).

Мета обробки персональних даних має бути:

– сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних;

– відповідати законодавству про захист персональних даних (ч. 1 ст. 6 Закону № 2297 [137]).

Загальні вимоги до обробки і захисту персональних даних суб'єктів персональних даних визначає Типовий порядок обробки ПД [128]. Зокрема, Типовий порядок обробки ПД [128] скеровує, що володілець повинен визначити:

1) мету та підстави обробки персональних даних;

2) категорії суб’єктів персональних даних;

3) склад персональних даних;

4) порядок обробки персональних даних —

– спосіб збору, накопичення;

– строк та умови зберігання;

– умови та процедуру зміни, видалення або знищення;

– умови та процедуру передачі;

– перелік третіх осіб, яким можуть передаватися;

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

– заходи забезпечення захисту;

– процедуру збереження інформації про операції, пов’язані з обробкою персональних даних та доступом до них (п. 2.1 Типового порядку обробки ПД [128]).

Визначити все, що вимагає Типовий порядок обробки ПД [128], можна тільки в локальному нормативному акті. Як його назвати, ані Закон № 2297 [137], ані Типовий порядок обробки ПД [128] не регламентують. Це може бути положення, порядок, інструкція тощо, головне — документ має бути на підприємстві. Відтак, ми пропонуємо розроблений нами проєкт такого документу (Додаток А).

Контролює додержання законодавства про захист персональних даних Уповноважений ВР з прав людини (ст. 23 Закону № 2297 [137]). Порядок контролю затверджений наказом Уповноваженого ВР з прав людини від 08.01.2014 № 1/02-14 [128].

Якщо на підприємстві немає локального нормативного акта, який визначає все, що передбачено Законом № 2297 [137] та Типовим порядком обробки ПД [128], служба омбудсмена вручить припис на усунення порушень. Тобто зобов’яже розробити та затвердити документ.

Якщо через відсутність закріплених процедур орган контролю виявить порушення у сфері захисту персональних даних, що призвели до незаконного

доступу, знищення чи втрати персональних даних, посадових осіб притягнуть до адміністративної відповідальності.

Нормативні акти не передбачають прямої відповідальності, якщо роботодавець не обліковує операцій, пов’язаних із персональними даними. Якщо під час перевірки виявлять, що кадрова служба не веде обліку, складуть припис про усунення порушень. Якщо роботодавець не обліковує операцій і при цьому порушив права працівника як суб’єкта персональних даних, винній особі загрожуватиме адміністративна відповідальність у розмірі 300–1000 нмдг (ст. 188-39 КУпАП [96]). Наразі жодну особу не притягнули до адміністративної відповідальності через цей прецедент.

### 1.3. Міжнародна практика захисту персональних даних на підприємствах

Джерела міжнародно-правового регулювання захисту персональних даних можна об'єднати у три групи. Першу групу складають нормативні акти декларативного характеру, що охороняють честь та гідність. З ними тісно пов'язані норми, спрямовані на захист особи від дискримінації.

Друга група містить норми про міжнародний інформаційний обмін. До неї також належать акти, що регулюють інформаційне забезпечення єдиного ринку трудових ресурсів. До них теж доречно віднести акти про правове становище міжнародних бюро та агентств зайнятості.

Третя група актів містить норми, що регламентують захист приватного життя людини. Це міжгалузеві правові акти, які забезпечують недоторканність приватного життя у різних сферах її прояву. Частина нормативних джерел цієї групи спрямована на безпосередній захист персональних даних працівника. Норми про використання та охорону персональних даних працівників організації можуть міститися в колективному договорі, у правилах внутрішнього трудового розпорядку, у положеннях про захист конфіденційної інформації та захист персональних даних працівників, про доступ до

електронної пошти, у положеннях про структурні підрозділи організації, посадових інструкціях співробітників, які мають право доступу до персональних даних, та в інших нормативних правових актах організації [86, с. 14-15].

Наразі у практиці ЄС сформована розгалужена система міжнародних актів у формі декларацій, конвенцій, рекомендацій, у яких знайшли відображення засадничі європейські принципи у сфері захисту персональних даних особи. До них, зокрема, належать: Загальна декларація прав людини 1948 року [92]; Конвенція про захист прав і основоположних свобод людини 1950 року [99]; Конвенція про захист осіб у зв'язку з автоматизованою обробкою їх персональних даних 1981 року [98]; Додатковий протокол до Конвенції щодо наглядового органу та транскордонних потоків даних 2001 року [89]; Рекомендації Комітету міністрів Ради Європи про захист персональних даних, що застосовуються у сфері найму (1989 рік) [62]; Рекомендації Комітету міністрів Ради Європи щодо захисту персональних даних особи у зв'язку з працевлаштуванням 2015 року [61]; Рекомендації Комітету міністрів Ради Європи № R (87) 15 щодо використання персональних даних у сфері діяльності правоохоронних органів 1987 року [150], Рекомендації Комітету міністрів Ради Європи № R (97) 5 щодо захисту медичних даних 1997 року [151] тощо. Однак головна проблема у сфері захисту персональних даних в Україні полягає у відсутності законодавчих актів, які забезпечували б належний рівень захисту персональних даних в Україні у відповідності до оновлених міжнародних стандартів у цій сфері [105, с. 31-32].

Підписавши Угоду про асоціацію з Європейським Союзом, Україна погодилась на співробітництво з ЄС з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи, як це передбачено статтею 15 Угоди [106, с. 84].

Майже одразу після 2000 року, Директива 95/46/ЕС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних

і про вільне переміщення таких даних» (далі – «Директива») вже не могла справлятися з новими викликами, які з'явились разом з новою технологічною індустрією, яка динамічно розвивалась. Персональні дані суб'єктів персональних даних використовувались не тільки для потреб бізнесу. Все більше і більше процесів з обробки даних та невизначеностей виникало у сфері соціальних медіа, що і спричинило неминуче створення нового підходу до захисту персональних даних.

До створення GDPR, всі країни-члени ЄС та Європейської Економічної Зони (далі – «ЄЕЗ») імплементували Директиву в своє національне законодавство, але зі значною різницею у предметі регулювання. Це призвело до багатьох труднощів, як для зростаючої кількості міжнародних бізнесів, так і для регуляторів, які мали здійснювати захист на єдиному європейському рівні [35].

Поява GDPR пов’язана насамперед із розвитком IT-технологій та інтернету. Технології дають змогу як приватним підприємствам, так і публічним органам збирати персональні дані та користуватися ними у безпрецедентних масштабах. Зворотна сторона прогресу – економічні та соціальні ризики для фізичних осіб. Витік персональних даних може спричинити фінансові махінації, тиск на особу або маніпулятивні впливи [108, с. 179].

7 грудня 2000 року Хартія Європейського Союзу про основні права (далі – «Хартія ЄС») вступила в силу, де у ст. 8 [171] передбачено захист персональних даних як права людини. Принципи Хартії ЄС про персональні дані також були втілені в Лісабонській угоді від 13 грудня 2009 [90].

4 листопада 2010 року Європейська комісія опублікувала стратегію посилення процесу захисту даних на європейському рівні [91]. У січні 2012 року Європейська комісія підтвердила комплексний план реформ, у тому числі необхідність заміни Директиви на Регламент ЄС, який буде встановлювати єдині вимоги у всьому ЄС [97]. У 2012 році 29WP опублікувала два заключення, що стосуються цього зазначеного плану реформ [51].

GDPR досить довго розроблявся спільно Європейською комісією, Європейським парламентом і Радою ЄС і був опублікований в Офіційному Журналі ЄС у квітні 2016 року, за два роки до набрання ним чинності – 25 травня 2018 року.

Обробка даних у контексті працевлаштування підпадає під загальне законодавче регулювання ЄС питань захисту персональних даних. Однак один

Регламент [2] конкретно стосується захисту обробки персональних даних Європейськими інституціями в контексті працевлаштування (серед інших питань). У Загальному регламенті захисту персональних даних трудові відносини згадуються у ст. 9 (2), де зазначено, що персональні дані можуть оброблятися під час виконання обов'язків чи реалізації окремих прав контролера чи суб'єкта даних у сфері зайнятості.

Відповідно до Загального регламенту захисту персональних даних, працівник повинен мати можливість чітко виокремлювати дані, на обробку/зберігання яких він/вона погоджується, та цілі, з метою яких його/її дані зберігаються. Працівники також до моменту надання згоди мають бути поінформовані про свої права та тривалість зберігання їхніх даних. У разі витоку персональних даних, що може призвести до високого ризику для прав і свобод фізичних осіб, роботодавець має повідомити про цей витік працівника. Стаття 88 Регламенту дозволяє державам-членам запроваджувати конкретніші правила для забезпечення захисту прав і свобод працівників щодо їхніх персональних даних у контексті працевлаштування.

У справі «Вортен» [170] дані включали записи робочого часу, що містили інформацію про щоденні періоди роботи та періоди відпочинку, які є персональними даними. Національним законодавством може вимагатися надання роботодавцем доступу до записів робочого часу державним органам, що здійснюють моніторинг умов праці. Це дозволяє отримати негайний доступ до відповідних персональних даних. Однак доступ до персональних даних є необхідним для надання можливості національним органам здійснювати контроль за дотриманням законодавства щодо умов праці.

Що стосується РЄ, то 1989 року була видана, а 2015 року переглянута Рекомендація щодо даних працевлаштування [61]. Рекомендація охоплює обробку персональних даних в цілях працевлаштування, як у державному, так і приватному секторі. Обробка має відповідати певним принципам та обмеженням, таким як принцип прозорості та консультації з представниками працівників перед встановленням системи нагляду на робочому місці. У Рекомендації також зазначено, що роботодавці повинні застосовувати превентивні заходи, наприклад замість відстеження, як їхні працівники користуються Інтернетом, застосовувати фільтри.

Огляд найпоширеніших проблем захисту персональних даних, характерних для контексту працевлаштування, можна знайти в робочому документі Робочої групи «Стаття 29» [162]. Робоча група проаналізувала значення згоди як правової підстави для обробки даних про зайнятість [162]. Вона виявила, що відсутність економічної рівноваги між роботодавцем, який просить згоди, і працівниками, які надають її, часто викликає сумніви щодо того, чи було цю згоду надано вільно. У зв'язку з цим, оцінюючи дійсність згоди в контексті працевлаштування, необхідно уважно розглянути умови, за яких згода використовується як юридична підстава обробки даних.

Загальною проблемою захисту персональних даних у нинішньому типовому робочому середовищі є обсяг правомірного контролю за електронною комунікацією працівників на робочому місці. Часто стверджують, що цю проблему можна легко вирішити шляхом заборони використання засобів зв'язку на роботі у приватних цілях. Однак така загальна заборона може бути непропорційною і нереальною. У цьому контексті особливо цікавими є рішення ЄСПЛ у справах «Копланд проти Сполученого Королівства» та «Барбулеску проти Румунії».

У справі «Копланд проти Сполученого Королівства» [157] за використанням працівницею коледжу телефону, електронної пошти та інтернету здійснювався прихований контроль з метою з'ясування, чи було з її боку надмірним використання обладнання коледжу в особистих цілях.

ЄСПЛ постановив, що телефонні дзвінки, здійснені у службових приміщеннях, підпадають під поняття приватного життя і таємницю кореспонденції. Тому такі дзвінки та електронні листи, надіслані з роботи, а також інформація, отримана в результаті моніторингу персонального використання інтернету, захищені статтею 8 ЄКПЛ. У справі заявниці не існувало жодних положень, які регламентували б обставини, за яких роботодавці можуть відстежувати використання працівниками телефону, електронної пошти та інтернету. Таким чином, втручання не відповідало закону. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

У справі «Барбулеску проти Румунії» [156] заявника було звільнено за використання Інтернету за місцем його роботи в робочий час з порушенням внутрішніх правил. Роботодавець відслідковував його комунікації. Під час провадження в суді країни були представлені записи, які відображали повідомлення суто приватного характеру. Встановлюючи застосовність статті 8, ЄСПЛ лишив відкритим питання, чи міг заявник достатньою мірою очікувати на конфіденційність з огляду на встановлені роботодавцем обмежувальні правила, однак Суд постановив, що правила роботодавця не можуть зводити нанівець приватне соціальне життя на робочому місці.

Щодо суті, Договірні Сторони повинні мати свободу розсуду у визначенні необхідності запровадження нормативних документів, які обумовлюватимуть умови, за яких роботодавець може регламентувати електронні чи інші комунікації непрофесійного характеру своїх працівників на робочому місці. Проте національні органи повинні були забезпечити, щоб запровадження роботодавцем заходів щодо моніторингу листування та інших комунікацій, незалежно від обсягу та тривалості таких заходів, супроводжувалося належними та достатніми гарантіями проти зловживань.

Пропорційність та процедурні гарантії проти свавілля є дуже важливими, і ЄСПЛ визначив низку факторів, що були суттєвими в даних обставинах. До них належать, серед іншого, обсяг перевірки роботодавцем і ступінь втручання в приватне життя працівника, наслідки для працівника, та чи були забезпечені належні гарантії. Крім того, національні органи мали

забезпечити, щоб працівник, спілкування якого відстежувалося, мав доступ до захисту в суді, що мав би повноваження визначати, щонайменше по суті, яким чином було дотримано зазначених критеріїв та чи були оскаржувані заходи правомірними.

У цій справі ЄСПЛ встановив порушення ст. 8, оскільки національні органи не надали належного захисту праву заявника на повагу до приватного життя і кореспонденції, внаслідок чого не змогли досягти справедливого балансу між інтересами, що розглядалися.

Відповідно до Рекомендації РЄ щодо даних про працевлаштування, персональні дані, що збираються в цілях працевлаштування, повинні бути отримані безпосередньо від працівника.

Персональні дані, що збираються для найму, повинні обмежуватися інформацією, необхідною для оцінки придатності кандидатів та їхнього кар'єрного потенціалу.

У Рекомендації також окремо вказано на оціночні дані, які стосуються продуктивності або потенціалу окремих працівників. Оціночні дані повинні ґрунтуватися на справедливих та чесних висновках і не повинні бути образливими у своєму формулюванні. Цього вимагають принципи чесної обробки і точності даних.

Особливим аспектом законодавства щодо захисту персональних даних у відносинах між роботодавцем і працівниками є роль представників працівників. Такі представники можуть отримати персональні дані працівників лише в обсязі, необхідному для того, щоб мати можливість представляти інтереси працівників, або якщо такі дані необхідні для виконання чи контролю за зобов'язаннями, передбаченими колективними договорами.

Чутливі дані, зібрані в цілях працевлаштування, можуть оброблятися лише в окремих випадках і згідно з гарантіями, передбаченими в національному законодавстві. Роботодавці можуть запитувати працівників або кандидатів на посаду про стан їхнього здоров'я або організовувати їхній медичний огляд лише за необхідності. Це може бути зроблено для визначення

придатності для працевлаштування, дотримання вимог профілактичної медицини, захисту життєво важливих інтересів суб'єкта даних чи інших працівників та фізичних осіб, надання дозволу на призначення соціальних пільг чи надання відповіді на судові запити. Дані про стан здоров'я не можуть збиратися з інших джерел, окрім як отримуватися від відповідного працівника, за винятком випадків, коли було отримано явно висловлену та поінформовану згоду, або якщо це передбачено національним законодавством.

Згідно з Рекомендацією щодо даних про працевлаштування, працівники повинні бути поінформовані про мету обробки їхніх персональних даних, тип

персональних даних, що збираються, суб'єктів, яким регулярно повідомляються дані, мету та правову підставу такого розкриття. Доступ до електронних комунікацій на робочому місці може здійснюватися лише з міркувань безпеки чи з інших легітимних підстав, і дозволяється лише після інформування працівників про те, що роботодавець може мати доступ до такого способу спілкування.

Працівники повинні мати право на доступ до своїх даних щодо працевлаштування, а також право на їх виправлення чи видалення. Якщо обробляються оціночні дані, працівники також повинні мати право на оскарження цієї оцінки. Втім, ці права можуть тимчасово обмежуватися з метою проведення внутрішніх розслідувань. Якщо працівнику було відмовлено в наданні доступу, виправленні або видаленні персональних даних щодо працевлаштування, національне законодавство має передбачати належні процедури оскарження відмови [114, с. 357-361].

Цікавим є дослідження зарубіжного досвіду європейських держав. підхід ЄС до забезпечення захисту персональних даних базується на розвитку «цифрових знань» і «цифрової грамотності», які мають підвищити рівень безпеки обороту персональних даних в цифровому середовищі [49, с. 37]. Трудове законодавство деяких держав-членів безпосередньо стосується питання конфіденційності. Але такі країни-члени скоріше залишаються винятком, а ці ініціативи є нещодавніми або знаходяться на стадії підготовки.

Досить унікальним випадком є Фінляндія, яка прийняла Закон про захист приватного трудового життя (далі – Закон про конфіденційність зайнятості) [1]. Цей закон був кроком до зміцнення підходу до секторального регулювання. Завдяки своїй відносно широкій сфері дії акт був своєрідною піонерською спробою в межах ЄС. Під час підготовки Закону про конфіденційність зайнятості, схожі моделі правового регулювання були представлені в інших країнах Європи, наприклад у Франції з так званим «законом Обрі» 1993 р. [69] і в Данії – законом про дані про стан здоров'я в трудовому житті [9]. Але у Фінляндії підхід набагато ширший. Також в Іспанії Статут працівників 1995 року присвячує деякі свої статті темі захисту приватності і гідності працівника, але він не пропонує повного та послідовного поводження з метою захисту приватності працівника. Ще один акт з відносно широким підходом до правовим регулюванням збору та обробки персональних даних у трудовому житті готується у Швеції [34, с. 13].

Прийняття Закону про конфіденційність трудових відносин у Фінляндії викликано потребою в спеціальному регулюванні трудової діяльності, адже існуючий Закон про захист даних не міг повністю задовольнити особливі потреби регулювання відносин у сфері зайнятості. Саме тому Закон про конфіденційність трудових відносин доповнює Закон про захист даних, і навіть має пріоритет над цим законом у разі конфлікту норм.

Закон про конфіденційність трудових відносин містить загальні положення щодо збору та обробки даних про співробітників. Крім того, існують положення про особистісні тести, оцінювання, медичні тести, включаючи тестування на алкоголь і наркотики та генетичне тестування. Нарешті є приписи про технічний нагляд, моніторинг електронної пошти та інших телекомунікацій.

Регулятивний підхід в акті різноманітний. Правила мають переважно загальний характер, а також визначають стандарти якості та альтернативні, правила чи процедури. Деякі з них є на додаток до положень іншого законодавства або звичаїв, затверджених судовою практикою. Наприклад, формальна компетенція роботодавця вимагати перевірки стану здоров'я чи

перевірки на наркотики не є такою залежно від Закону про конфіденційність трудових відносин. Вважається, що цей спосіб регулювання частково залежить від характеру об’єкта регулювання, частково від складності співставлення двох чи кількох полів регулювання та частково щодо можливостей пошуку політичного рішення. Коли парламент Фінляндії прийняв Закон про конфіденційність трудових відносин, він вимагав усунути деякі прогалини в законі. Відтак, Міністерство праці створило комісію для аналізу ситуації і, якщо необхідно, окремо підготувати законодавство про тестування на наркотики саме в трудовій діяльності.

У Швеції Закон про захист особи і її репутації у трудовому житті базується на Законі про персональні дані і є спеціальним актом, що означає, що у відповідних випадках його положення будуть застосовуватися в аспекті Закону про персональні дані. Зазначений Закон також охоплює методи здійснення різних заходів, які можуть включати порушення особистої недоторканності працівника. Визначено, зокрема, що персональні дані в першу чергу збираються від самого працівника. Тільки в тих випадках, коли це неможливо, роботодавець може за згодою працівника збирати інформацію з деяких інших джерел.

Крім того, щоб захистити особисту свободу працівника, закон визначає спосіб проведення медичних оглядів, тестів на наркотики та встановлює перелік особистісних тестів, які можуть бути проведені. Цей закон про захист особи і її репутації у трудовому житті стосується як державного, так і приватного секторів економіки. Його мета полягає в тому, щоб посилити захист не тільки чесності співробітника, але й захистити недоторканність претендентів на роботу та колишніх працівників.

В Іспанії Закон про працівників 1995 року (ES) [65] посилається на право на недоторканність приватного життя та гідність працівників. Крім того, Закон від 8 листопада №13/1995 [6] про запобігання ризиків у сфері праці встановлює, що роботодавець гарантує своїм працівникам періодичне обстеження їх стану здоров'я залежно від невід'ємних ризиків для роботи, маючи на увазі, що спостереження за станом здоров'я працівників буде

здійснюватися, як правило, за їх попередньою згодою та, поважаючи право працівника на приватне життя та його гідність, а також конфіденційність усієї інформації, пов'язаної з його станом здоров'я. Також у сфері трудового права законодавчий декрет від 4 серпня 2000 р. № 5/2000 дії роботодавця, що суперечать дотриманню конфіденційності та не враховують гідність працівника розглядаються як серйозні порушення, і карається штрафом від 3,00 до 90 000 євро.

У Франції Трудовий кодекс містить положення про конфіденційність працевлаштування. Конкретні Правила були прийняті ще в 1992 році після публікації доповіді професора *G. LyonCaen*, який досіджував комп'ютеризовані форми моніторингу працівників. Та доповідь підкреслювала ризики застосування нових технологій для особистої свободи на роботі. Після презентації цього звіту до закону було внесено зміни та окремі положення були прийняті щодо моніторингу працівників та обробки даних працівників.

В Італії найважливішим джерелом регулювання є Трудовий статут 1970 року, який регулює трудові відносини в Італії [70]. Він містить правила для захисту свободи та гідності працівників і свободи профспілок та їхню діяльність на робочому місці [33]. Таким чином, Статут установлює вузькі межі управлінських прерогатив, щоб захистити працівника, його гідність та приватне життя [11]. Наприклад, визнається незаконним для роботодавця проводити розслідування для з'ясування даних, збирання інформації про політичні, релігійні позиції, участь у профспілках працівника або факти, які не мають відношення до оцінки працівника в аспекті виконуваної роботи під час працевлаштування або вже у ході трудових відносин.

Зупинимося на деталях правового регулювання захисту персональних даних працівників у певних країнах-членах ЄС. Так, перший федеральний закон ФРН про захист персональних даних, *Bundesdatenschutzgesetz* (далі – BDSG – Федеральний закон про захист даних) був прийнятий ще у 1977 р. Наступним кроком для розвитку законодавства щодо захисту персональних даних послужила справа перепису населення – *Volkszählungsurteil*.

*Bundesverfassungsgericht* (Федеральний конституційний суд) постановив, що *Grundgesetz* (Основний закон, тобто Конституція Німеччини) не лише захищає конфіденційність як таку, але й повагу до приватного життя людини, що охоплює захист персональних даних. Таким чином, Конституція передбачає певний ступінь правового захисту персональних даних [57, с. 5].

Розвиток економіки, основаної на інноваційних знаннях, технологічних прогрес і зростаюча роль людському капіталу, посилили збір персональних даних працівників у контексті працевлаштування. Ці події породжують низку занепокоєнь і ризиків, а тому ставить питання ефективного захисту особистих даних працівників.

Із з прийняттям Директиви 95/46/ЄС про охорону фізичних осіб щодо обробки персональних даних і вільного переміщення таких даних (Директива про захист даних), Закон про захист даних був гармонізований з європейським законодавством. Однак все рівно повсякчас виникають дискусійні питання – як знайти баланс між зрозумілим бажанням працівника конфіденційності – з одного боку та життєво важливих інтересів роботодавця – з іншого, наприклад, попередження злочинів або будь-яких інших порушень, встановлених для його фірми за допомогою відеоспостережень, тощо. Забезпечення пропорційності між цими протилежними принципами має першочергове значення для тлумачення положень про захист даних в контексті трудового права, незалежно від того, чи це європейські чи національні норми.

Структура закону про захист даних ФРН проста і сувора: уся обробка персональних даних працівників повинна бути обґрунтована. Що стосується національного закону про захист даних, цей принцип закріплено в розділі 4 (1) Федерального закону ФРН про захист даних (*Bundesdatenschutzgesetz,* далі – *BDSG*). Відповідно до цього закону збирання, переробка і використання персональних даних є законним, лише якщо це дозволено або передбачено цим Законом чи іншим законодавством або якщо суб’єкт даних надав згоду. Цей принцип стосується не лише державних органів, таких як поліція, але також обмежує використання персональних даних приватними особами, такими як

роботодавець. Отже, кожен роботодавець повинен обґрунтувати всі збори, обробку та використання персональних даних працівників.

Відповідно до розділу 4 (1) BDSG існує три допустимі підстави для обґрунтування збору, обробки та використання персональних даних працівників:

– обробка дозволена відповідно до BDSG;

– обробка дозволена іншим законом, що стосується питань захисту даних, або суб'єкт даних (тобто працівник) дав свою згоду.

Закон про захист даних базується на певних принципах, які є керівними вимогами при обробці персональних даних у трудових відносинах. Ці принципи викладено у висновку 2001 року Робочої групи у ст. 29 щодо обробки персональних даних в контексті працевлаштування, це зокрема:

1) остаточність, тобто дані повинні збиратися для конкретної, чіткої та законної мети і не оброблятися в подальшому способом, несумісним з цими цілями;

2) прозорість – працівники повинні знати, які дані роботодавець збирає про них (безпосередньо або з інших джерел), які є цілі щодо обробки, передання або використання цих даних у даний момент або в майбутньому. Прозорість також забезпечується наданням права суб'єкту даних на доступ до його/її особистих даних і зобов'язання контролерів даних повідомляти наглядові органи, як це передбачено національним законодавством;

3) законність – обробка персональних даних працівників має бути законною. Стаття 7 Директиви перераховує критерії згідно із якими обробку визнають законною;

4) пропорційність – особисті дані мають бути адекватними, релевантними та не містити надмірностей щодо цілей, для яких вони збираються та/або оброблюються. Припускаючи, що працівників було поінформовано про обробку та, що така діяльність з обробки є законною та пропорційною, все ж обробка має бути справедливою щодо працівника;

5) точність та зберігання даних: відомості у трудових книжках повинні бути точними та, де необхідно, оновлюватися. Роботодавець повинен вжити

заходів, щоб переконатися, що дані неточні або неповні, беручи до уваги цілі, для яких вони були зібрані або оброблені, видаляються або виправляються;

6) принцип безпеки проявляється у тому, що роботодавець повинен запровадити відповідні технічні та організаційні заходи на робочому місці, щоб гарантувати, що особисті дані його працівників охороняються. Особливий захист повинен бути наданий щодо несанкціонованого розкриття даних або доступу до них чи серверів, на яких вони зберігаються;

7) обізнаність персоналу: персонал, відповідальний за обробку персональних даних інших працівників повинен знати про захист даних і отримати належне навчання. Без належної підготовки персоналу про поводження з особистими даними працівників, ніколи не може бути досягнуто належної поваги до приватного життя працівників на робочому місці.

У ФРН нормативне регулювання захисту персональних даних працівників складає законодавство ЄС та національне право. У разі конфлікту між різними положеннями, право ЄС має вищу силу: національне право, яке порушує європейське первинне право (яке є правом договорів), не може застосовуватися на національному рівні. Все національне законодавство має застосовуватися та тлумачитися судами (наскільки це можливо) у відповідності до права ЄС, незалежно від того, первинне чи вторинне це право. Тому спочатку варто керуватися правом ЄС, щоб зрозуміти систему захисту персональних даних ФРН.

Первинне право Євросоюзу приділяє велику увагу захисту конфіденційності громадян, персональних даних і повноважень щодо захисту персональних даних, як це можна побачити з приписів Хартії про основні права.

Відповідно до абз. 1 ст. 6 Договору про Європейський Союз Хартія про основні права є частиною основного закону Союзу. У ст. 8 Хартії ЄС визначено чіткі гарантії захисту персональних даних, зокрема:

1. Кожен має право на захист персональних даних, які його стосуються.

2. Такі дані повинні оброблятися справедливо для певних цілей і на основі згоди відповідної особи або іншої законної підстави, встановленої законом.

Кожен має право доступу до даних, які були зібрані стосовно нього, і право на їх виправлення.

3. Дотримання цих правил підлягає контролю з боку незалежного органу.

На рівні вторинного законодавства ЄС Директива 95/46/ЄС про охорону фізичних осіб щодо обробки персональних даних і вільного переміщення таких даних (Директива про захист даних) є центральним інструментом, що регулює обробку персональних даних. Ця Директива була розроблена і повинна тлумачитися відповідно до права європейських договорів, зокрема ст. 8 Хартії основних прав ЄС. Директива про захист даних поширюється на всю автоматизовану обробку персональних даних за винятком певних сфер, наприклад, національна безпека чи оборона, і обробка даних фізичною особою в ході суто особистої або домашньої діяльності. При цьому Директива регулює не тільки обробку даних приватними особами, зокрема обробку даних у комерційних умовах, а також обробку даних державними агентами, наприклад, у сфері правоохоронної діяльності або соціальної безпеки. Оскільки Директива про захист даних не містить спеціальних правил обробки даних про працівника роботодавцем, застосовуються загальні правила обробки під час відносин з працевлаштування та в ході трудових правовідносин.

Таким чином, Директива обов’язково вимагає національного імплементаційного акта, який тоді безпосередньо застосовується в цій державі-члені. Директива про захист даних має особливість імплементуватися не одним, а декількома імплементаційними актами Німеччини як на федеральному рівні, так і на рівні землі, які окремо покривають лише частину сфери дії Директиви.

Обробка даних приватними особами, а також обробка даних федеральними агентствами охоплюється *Bundesdatenschutzgesetz*

(*Федеральний закон про захист даних, BDSG*). Обробка даних агенціями федеральних земель, наприклад, для правоохоронних цілей, регулюються відповідними державними законами про захист даних. На практиці *BDSG* є найбільш важливим імплементаційним актом, оскільки охоплює обробку даних приватними особами.

Незважаючи на тривалість і безліч цих імплементаційних актів, держави-члени ЄС фактично мають дуже обмежену свободу дій у визначенні законності обробки персональних даних. Адже Директива встановлює базовий стандарт, але має на меті узгодити, як можна зрозуміти з її назви захист персональних даних із вільним потоком даних у межах спільного ринку. А щоб встановити єдині правила для спільного ринку, Директива 95/46/ЄС встановлює єдиний європейський стандарт, від якого країни-члени ЄС не можуть відступати ані в бік установлення суворіших правил, ані в бік їх послаблення, принаймні до тих пір, поки Директива належним чином не імплементована в національне законодавство однаково для всіх держав-членів ЄС.

Статті 6 і 7 Директиви містять найважливіші положення щодо істотних стандартів права. Стаття 6 встановлює принципи, що стосуються якості даних:

1. Держави-члени передбачають, що персональні дані повинні:

(a) оброблятися чесно та законно;

(b) збиратися для визначених, явних і законних цілей і не оброблятися у спосіб, несумісний з цими цілями. Подальша обробка даних для історичних, статистичних чи наукових цілей не вважаються несумісними за умови, що Держави-члени забезпечують відповідні гарантії;

(c) бути адекватними, відповідати цілям, для яких вони призначені, зібрані та/або обробляться;

(d) бути точним і, за необхідності, оновлюватися; необхідно вжити всіх розумних кроків, щоб гарантувати, що дані, які є неточними або неповними, враховували цілі для яких вони були зібрані, або для яких вони далі обробляються, видаляються або виправляються (це так званий принцип обмеження мети);

(e) зберігатися у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це є необхідним для цілей, для яких дані були зібрані або для яких вони призначені та далі обробляються. Держави-члени встановлюють належні гарантії для особи щодо даних, що зберігаються протягом тривалого часу для історичного, статистичного чи наукового використання.

Принцип обмеження мети полягає у тому, що дані можуть бути оброблені лише для певних цілей і лише настільки, наскільки це необхідно для досягнення цієї мети. Це зобов'язує особу, яка контролює обробку даних відобразити його дії з обробки та чітко визначити цілі.

Обробка персональних даних має відбуватися законно, що означає те, що будь-яка обробка потребує чіткої правової основи, а правові підстави обробки перелічені в ст. 7 Директиви про захист даних, зокрема:

Держави-члени передбачають, що персональні дані можуть оброблятися, лише якщо:

(a) суб'єкт даних однозначно дав свою згоду;

(b) обробка необхідна для виконання контракту, укладеного суб'єктом даних зі стороною або для того, щоб вжити заходів для відповіді на запит суб'єкта даних до укладення контракту;

(c) обробка необхідна для дотримання юридичних зобов'язань, які виконує контролер;

(d) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних;

(e) обробка необхідна для виконання завдання, яке виконується в суспільних інтересах або під час виконання офіційних повноважень, наданих контролеру або третій стороні, якій розкриваються дані;

(f) обробка необхідна для дотримання законних інтересів, яких переслідує контролер або третя сторона або сторони, яким дані розкриваються, за винятком випадків, коли такі інтереси превалюють над основними правами і свободами суб'єкта даних, який потребує захисту.

Баланс інтересів може порушитися лише на користь контролера, оскільки цей баланс інтересів можна оцінити лише в окремому випадку на

основі конкретного випадку, відтак імплементаційні акти, які взагалі забороняють певні види обробки, є цілком достатніми для приватного сектору. Навряд чи можна вважати, що баланс інтересів завжди буде на користь особи, чиї дані обробляються.

Тому в багатьох випадках імплементаційні акти повинні тлумачитися досить широко, щоб відповідати стандарту Директиви. Директива не лише вимагає Державам-членам прийняти імплементаційні акти відповідно до Директиви, а також вимагає їх тлумачити відповідно до Директиви. Тим не менш, у межах її дії вплив Директиви є дуже далекосяжним, адже навіть якщо особисті дані можуть бути захищені конституціями держав-членів, як це має місце в Німеччині, все ж ці Положення також повинні тлумачитися відповідно до Хартії ЄС про основні положення права та Директива. Маючи на увазі, що сама Директива встановлює баланс між захистом персональних даних і, зокрема, комерційними інтересами, цей баланс має бути перенесено до національних конституцій, адже наразі незрозуміло наскільки держави-члени мають свободу дій у визначенні балансу.

Суд Європейського Союзу (СЄС) і його тлумачення Директиви не залишає великого простору для маневру для Держав-членів. У своїй справі *Lindqvist* [27] Суд постановив, що гармонізація національного законодавства не обмежується мінімальною гармонізацією, а є лише гармонізацією, яка загалом є повною. Директива 95/46 дозволяє Державам-членам кроки для маневру в певних сферах і дозволяє їх підтримувати або вводити конкретні правила для конкретних ситуацій, як демонструє велика кількість його положень. Однак такі можливості повинні використовуватися у спосіб, передбачений Директивою 95/46 і відповідно до своєї мети підтримувати баланс між вільним переміщенням персональних даних і захистом приватного життя.

У ФРН визначено, що збір, обробка та використання персональних даних є законними, лише якщо це дозволено або передбачено законом, або якщо суб’єкт даних надав згоду. У контексті зайнятості найважливіше положення, яке служить основою для обґрунтування обробки персональних даних є розділ

32 *BDSG*. У Розділі 32 *Bundesdatenschutzgesetz* (Федеральний закон про захист даних, *BDSG*) визначені правила збору, обробки та використання даних для цілей, пов'язаних із працевлаштуванням. Так, персональні дані працівника можна збирати, обробляти або використовувати для цілей, пов'язаних з працевлаштуванням, якщо це необхідно для прийняття рішень про наймання для виконання або розірвання трудового договору. Особисті дані співробітників можуть збиратися, оброблятися або використовуватися для розкриття злочинів лише за наявності документально підтверджених підстав, що суб'єкт даних вчинив злочин під час роботи, а відтак збір, обробка або використання таких даних необхідно для розслідування злочину, а не суперечить законному інтересу суб'єкта даних щодо виключення збору, обробки або використання, і, зокрема, тип і обсяг не є непропорційними причина.

Персональні дані працівників збираються, обробляються або використовуються без обробки за допомогою автоматичних процедур або обробки, використання в або з неавтоматизованих систем реєстрації, а також якщо не збираються в такій системі реєстрації з метою обробки або використання.

За таких умов приписи *Bundesdatenschutzgesetz* (Федеральний закон про захист даних, *BDSG*) дозволяють обробку даних лише в тій мірі, в якій це необхідно для прийняття рішень щодо найму, виконання або розірвання трудового договору. Це формулювання призвело до того, що іноді такий підхід тлумачать дуже вузько і, наприклад, виключають працівника від перевірки без конкретних підстав для підозри [5]. Однак цей підхід часто не відповідає Директиві, що стосується балансу між інтересами, який не обмежує обробку персональних даних працівників випадками, коли це необхідно. Одним із прикладів є вищезгадана перевірка працівників: обробка є лише незначним втручанням у конфіденційність співробітників, наприклад, автоматична перевірка платежів, які здійснюються компанією підрядникам, не сплачуються на той самий банківський рахунок, що й заробітна плата працівника, що може

бути виправдано переважним інтересом роботодавців про боротьбу із шахрайством в компанії.

Крім того, розділ 32 (3) BDSG розширює сферу захисту за межі сфери дії Директиви про захист даних, оскільки вона реалізує та включає також неавтоматизовані.

Окрім розділу 32 BDSG, ще одна важлива опція для обґрунтування обробки персональних даних у контексті працевлаштування є згода працівника. Як зазначено в Розділі 4 і 4a BDSG, згода є однією з підстав, за яких персональні дані можуть бути оброблені законно. Але що саме таке згода? Відповідно до ст. 2(h) Директиви 95/46/ЕС «згода суб'єкта даних означає будь-яку вільно надану конкретну та інформовану вказівку його/її побажання, якими суб'єкт даних підтверджує свою згоду на обробку персональних даних. З приписів Директиви 95/46/ЕС можна виокремити чотири вимоги, які мають бути виконані для надання згоди, зокрема:

– згода надається безкоштовно;

– згода має бути конкретною;

– та інформативною.

Охарактеризуємо кожну з ознак.

1. Згода надається безкоштовно. Цю умову можна вважати найбільш спірним поняттям в аспекті трудового права. Економічний тиск може бути прирівняний до примусу, щоб спотворити згоду [72]. З цим можна посперечатися в контексті працевлаштування, адже взагалі то згода ніколи не дається повністю вільно, адже так чи інакше працівник має вільний вибір – подавати документи чи ні [64].

Відповідно до чинного законодавства ЄС згода працівника не повинна автоматично узаконювати й обробку. Так, зокрема вирішив Європейський суд з прав людини (ЄСПЛ). Адже обробка все одно повинна відповідати іншим вимогам захисту даних, зокрема принципу пропорційності [32].

2. Згода має бути конкретною. Німецьке формулювання («*für den konkreten Fall*» – у конкретному випадку) пропонує обмеження легітимізації згоди працівника на певну обробку лише конкретних персональних даних.

Звідси вимога конкретності виключає все невизначене і узагальнені форми згоди, які легітимізують будь-яку обробку даних стосовно трудових відносин [64].

3.Згода має бути інформативною. Суб'єкт даних повинен знати про характер обробки та будь-які важливі особливості, які можуть вплинути на дані про нього/неї [55]. Це також означає, що суб’єкт даних повинен мати можливість оцінити наслідки його/її згоди щодо його/її основних прав. Особливо важливо, щоб суб'єкт знав, які персональні дані оброблятимуться та з якою метою. Щодо ступеня знань, які необхідні для того, щоб зробити згоду дійсною, можна провести паралелі з доктриною інформованої згоди, яка була розроблена для випадків недбалості щодо лікування [10; 41]; ці паралелі можуть бути особливо повчальними щодо обробки конфіденційних даних.

Важливим є те, що згода на обробку персональних даних працівника має включати вказівку на бажання суб’єкта даних. Тому мовчання чи просто пасивної згоди недостатньо [64]. З іншого боку, згода може бути виведена з поведінки, якщо вона є явною [25]. Відповідно до пункту (17) Директиви 2002/58/ЕС згода може бути надана будь-яким відповідним способом, що дозволяє вільно надавати конкретну та інформативну вказівку побажань користувача, в тому числі шляхом встановлення галочки під час відвідування на Інтернет-сайт. Відповідно до розділу 4a *BDSG*, згода суб’єкта даних має бути в письмовій формі.

Згода в контексті працевлаштування обмежується ситуаціями, коли працівник має вільний вибір і здатний відкликати згоду без перешкоди [53]. Однак досі залишається спірним, чи згода працівника може бути вільно надана в ситуаціях працевлаштування. Наприклад, якщо надання згоди є умовою найму, дуже ймовірно, що працівник прийме відповідне застереження, щоб не втратити можливість роботи [53]. Відтак, нерівність переговорів, підпорядкування, властиве трудовим відносинам, може змусити працівника надати згоду на обробку даних [54; 4; 47]. Із цієї причини німецький уряд обговорює реформу закону про захист даних, що призведе до скасування згоди на обробку персональних даних працівника у трудових відносинах [67].

А ось у Фінляндії Закон про захист приватності у трудовій діяльності передбачає, що роботодавець має право обробляти персональні дані лише у випадках, коли це є необхідним для дотримання прав і обов'язків сторін трудового договору; і ця умова не може змінюватися навіть за згодою працівника [8]. У Бельгії лише згода працівника не може бути легітимною підставою для обробки конфіденційних даних.

Захист даних у контексті працевлаштування стосується, перш за все забезпечення пропорційного балансу прав та інтересів між роботодавцем і працівником. Головне питання: як знайти баланс між зрозумілим прагненням працівника до приватності, з одного боку, і важливими для роботодавця інтересами – з іншого боку [71]?

Інтереси роботодавця можуть бути найрізноманітнішими. Поки є його/її мета законним, працівник теоретично може виправдати всю обробку персональних даних, доки роботодавець дотримується принципу пропорційності. Роботодавець може, наприклад, обробити дані з метою запобігання злочинам або будь-якому іншому порушенню правил, встановлених для його фірми засобами стеження, він/вона може обробляти дані для питань працевлаштування, ефективного управління людськими ресурсами, як-от: розподіл робочих місць, переведення працівників, дотримання правил охорони здоров’я та безпеки, спори про травми на виробництві та їх компенсацію, для запобігання витоку торгівлі таємниці, тощо. Тобто насправді незаконних цілей як таких мало, але не всі цілі, які переслідує роботодавець, мають однакову достовірність. Деякі цілі є важливіші за інші, і ці відмінності відображаються в структурі різних положень законодавства про захист даних. Наприклад, є спеціальний припис присвячений обробці персональних даних для розслідування злочинів (ст. 32(1) BDSG.

Директива про захист даних 95/46/ЄС також стосується певних типів персональних даних. Наприклад, положення про дані, які класифікуються як особливо чутливі, набагато суворіші. Розділ 3(9) BDSG визначає конфіденційні дані як будь-яку інформацію про расове або етнічне

походження, політичні погляди, релігійні або філософські переконання, членство в профспілках, здоров'я або статеве життя. Обробка цих конфіденційних даних має відповідати суворішим вимогам законодавства, ніж обробка інших даних. Розділ 28, наприклад, регулює обробку персональних даних у комерційних цілях. Відповідно до ст. 28(1) BDSG, персональні дані можуть оброблятися, «наскільки це необхідно для захисту законних інтересів контролера» і якщо «немає підстав припускати, що суб'єкт даних має переважний законний інтерес для виключення можливості обробки або використання».

Відповідно до розділу 28(6) BDSG збір, обробка та використання конфіденційних персональних даних є законними, лише якщо (а) необхідно для захисту життєво важливих інтересів суб'єкта даних або іншої особи, де суб'єкт даних фізично або юридично нездатний дати свою згоду, (б) йдеться про дані, які суб’єкт даних явно оприлюднив, (в) дані необхідні для ствердження, реалізації або захисту правових претензій, і немає підстав припускати, що суб'єкт даних має переважаючий законний інтерес у виключенні можливості збору, обробки чи використання, або (г) дані необхідні для цілей наукового дослідження, де науковий інтерес несе дослідницький проєкт значно переважає зацікавленість суб’єкта даних у виключенні можливість збору, обробки та використання, а мета дослідження не може бути досягнута будь-яким іншим способом або потребуватиме непропорційних зусиль.

Іншим прикладом відмінності між конфіденційними та іншими даними є положення про згоду суб’єкта даних. Загалом, згода має бути надана однозначно, а стосовно конфіденційних даних – суб'єкт даних повинен дати свою чітку згоду. Відтак, обробку «загальнодоступних даних» виправдати набагато легше, див. Розділ 28(1) BDSG або розділ 29(1) BDSG. Наведені приклади свідчать про те, що законодавець ФРН попередньо збалансував інтереси, що необхідно робити в кожному окремому випадку.

В усьому світі  під час пошуку роботи особи повинні бути готові відповісти на низку запитань ще до працевлаштування. Проте німецькі суди

обмежили право майбутнього роботодавця задавати питання [68]. Відповідно до судової практики, на співбесіді на роботе майбутній роботодавець може задавати питання лише тоді, коли він/вона має законну підставу знати відповідь. Якщо потенційний роботодавець задає питання, яке він/вона може не ставити, заявнику дозволено брехати, не боячись бути звільненим за брехню пізніше [20]. З 2009 року перевірка законних інтересів має законодавчу основу в розділі 32 Федерального Закону про захист даних. Згідно з цим правилом потенційний роботодавець може обробляти дані лише якщо обробка цих даних необхідна, тобто пропорційна. Крім того, розділи 19 Закону про генетичну діагностику (*Gendiagnostikgesetz*) визначають незаконною обробку даних заявників і співробітників (такі обмеження застосовуються з міркувань безпеки здоров'я). Нарешті, Загальний антидискримінаційний закон (*Allgemeines Gleichbehandlungsgesetz*) забороняє дискримінацію заявників на підставі расового або етнічного походження, статі, релігії або філософських переконань, інвалідності, віку або статевої приналежності та орієнтації. Якщо потенційний роботодавець обробляє дані щодо будь-якої з цих тем, це може свідчити про дискримінацію заявника. Тоді майбутній роботодавець повинен буде довести, що насправді він/вона не дискримінував особу, яка шукала роботу. На цьому тлі майбутній роботодавець має право просити претендента контактні дані, такі як його ім’я, адреса, номер телефону, водійські права тощо, якщо необхідна обробка цих даних. З іншого боку, роботодавець, зазвичай, не має права запитувати етнічну приналежність, походження або расову приналежність заявника, членство в профспілці, про інвалідність, хворобу (за умови, що це не становить загрози для оточуючих і не обмежує працездатність претендента), релігійні або філософські переконання (винятки можуть стосуватися релігійних груп як роботодавців), сексуальну орієнтацію, вагітність (оскільки це свідчить про дискримінацію за ознакою статі) [19] або членство в політичній партії.

Також роботодавець не має права запитувати будь-яким способом дані, які не стосуються можливих трудових відносин. Зазвичай, це стосується таких даних, як сімейний стан, кредитна інформація, історія судових процесів,

членство в клубі тощо. У деяких країнах потенційні роботодавці, вимагають від претендентів їхніх паролі у соціальних мережах. У ФРН це заборонено, більше того, спричинить громадський резонанс, а також адміністративні заходи у вигляді штрафів.

Роботодавцю може бути дозволено вимагати відомості про наявність/відсутність кримінальних судимостей або не знятих [20]. Однак він обмежується обробкою даних, які можуть вплинути на підбір майбутньої роботи та/або виконання її належним чином. Тому це може бути законним, приміром, для логістичної компанії запитати потенційного водія вантажівки, чи був він коли-небудь засуджений за злочини, пов’язані з дорожнім рухом, але їм не дозволено вимагати від нього, наприклад, судимості за образи людей. А ось фінансова установа може вимагати від претендента на посаду відомостей про судимості пов'язані з бізнесом (шахрайство, відмивання грошей тощо), але не чи був він засуджений, наприклад, за водіння в нетверезому стані. Завершені розслідування можуть бути перевірені, чи можуть вони обмежити здатність претендента отримати роботу або іншим чином вплинути на працевлаштування. Однак необхідно дотримуватись презумпції невинуватості, адже судова практика є досить обмежувальною щодо незавершених розслідувань [12].

Наразі відеоспостереження загальнодоступних місць або також приміщень приватних компаній широко використовується.

У ФРН використання систем відеоспостереження в основному регулюється трьома положеннями Федерального закону про захист даних (BDSG), на які роботодавець може покладатися, щоб обґрунтувати обробку персональних даних співробітників, за якими спостерігають камери:

– Розділ 6b BDSG: це положення регулює використання технологій відеоспостереження в загальнодоступних зонах, наприклад: супермаркети, вокзали, магазини тощо;

– Розділ 32 BDSG: ці положення застосовуються для нагляду за співробітниками у будь-якій іншій ситуації, тобто у закритих для громадськості місцях, таких як робоче місце;

– Розділ 28 BDSG: положення застосовується, якщо використовується відеоспостереження для цілей, не пов’язаних із трудовими відносинами, наприклад, коли клієнти або інші сторонні особи контролюються.

Усі ці положення вимагають законного інтересу чи мети для відео спостереження та тест на пропорційність. Цілі повинні бути конкретно обумовлені перед встановленням системи спостереження, тобто вони повинні бути задокументовані та доступні за допомогою процедур для будь-якої зацікавленої особи.

Головна причина, чому роботодавці встановлюють технології відеоспостереження, – це захист компанії проти вандалізму, крадіжок чи інших майнових злочинів або для захисту людей (співробітників, клієнтів тощо) від кримінальної діяльності. Так, загалом головне призначення відео стеження – це не моніторинг і контроль за працівниками. Однак і те, і інше часто на практиці поєднується. При цьому, в банках, в касах, працівники магазинів чи музеїв практично випадково також піддаються моніторингу. Однак хоч це випадково, хоч навмисно, а відеоспостереження за працівниками допустимо лише в суворих межах.

Незалежно від того, яке конкретне положення BDSG застосовується (чи Розділ 6b BDSG, що регулює використання відеоспостереження в загальнодоступних місцях, чи Розділ 28 BDSG, або Розділ 32 BDSG), коли йдеться про оцінку допустимість відеоспостереження, центральним критерієм оцінки завжди є тест на пропорційність. Має бути очевидно, що нагляд необхідний, тобто не має будь-якої іншої ефективної альтернативи окрім відеоспостереження. Крім того, співвідношення засобів і мети має бути пропорційним. Забороняється використовувати відеоспостереження у зв'язку з дрібними правопорушеннями, наприклад, з метою контролю за існуючою забороною на куріння. Якщо відеоспостереження загальнодоступних місць відповідає розділу 6b BDSG і ці загальнодоступні місця також є і робочими місцями, наприклад, відео спостереження в банку чи супермаркеті, де працівники теж знаходяться у зоні відео нагляду як властивості їх робочого місця. Однак у випадках, коли працівники є не реальним об'єктом

спостереження, то будь-яка оцінка результатів моніторингу для мети контролю продуктивності або інформації, пов'язаної з поведінкою, неприпустима. Тому оцінка відеоспостереження банку використовується з метою охорони, приміром, проти пограбування, буде виправданим, але не з метою контролю над поведінкою працівників. А ось в універмазі відеоспостереження, можливо, може бути законним, якщо використовується з метою захисту від учинення крадіжки працівниками.

Федеральний трудовий суд постановив, що навіть проста можливість стеження в будь-який час становить значний тиск на працівника, що є несумісним з його правом на повагу його/її особистих прав [14]. Федеральний трудовий суд зробив висновок, що відео нагляд на робочому місці виправданий лише у виняткових випадках, коли це робить роботодавець в життєвих інтересах. Загалом, слід припустити, що встановлено наступні принципи використання відео нагляду у судовій практиці:

а) перш ніж почати відеоспостереження, повинні бути достатні підстави для підозри (наприклад, у разі крадіжці, тощо), які виправдовують «вторгнення» в особисті права суб'єкта даних. А будь-якого розпливчастого припущення або загальної підозри щодо всіх працівників не достатньо, щоб встановити відео нагляд;

б) відеоспостереження, як правило, допустиме лише в тому випадку, якщо воно здійснюється відкрито, а не таємно, за допомогою видимих засобів і лише після того як співробітникам було надано достатню інформацію. Спостереження за допомогою прихованих камер допустиме, якщо це єдина можливість захистити законні інтереси роботодавця;

в) відеоспостереження є предметом спільного рішення робочої ради або персоналу ради;

г) результати незаконного моніторингу підлягають забороні на подальше використання. Вони також не можуть бути використані як доказ у позові про звільнення.

Використання Інтернету на роботі створює величезну кількість даних. З технологічної точки зору роботодавці можуть використовувати ці дані для

дослідження поведінки своїх працівників. Із юридичної точки зору, моніторинг використання Інтернету та таких програм, як електронна пошта співробітників викликає низку запитань. Вирішальним моментом є те, чи є таке спостереження підпадає під дію *Telekommunikationsgesetz* (Закон про телекомунікації, далі – TKG) чи ні. Так, якщо TKG застосовний, то роботодавцю дозволяється досліджувати використання Інтернету та електронної пошти, лише для технічних цілей (наприклад, сканування на віруси) і для розрахунків (якщо працівник повинен платити за приватне користування). TKG не дозволяє роботодавцю моніторингу даних, наприклад, з метою дотримання корпоративних вимог. Для роботодавців порушення TKG, ймовірно, становитиме злочин відповідно до розділу 206 *Strafgesetzbuch* (Кримінальний кодекс, StGB). Тому на практиці рекомендується діяти так, ніби TKG застосовний, навіть якщо це лише теоретичної точки зору.

Якщо TKG не застосовується, спостереження за використанням Інтернету та електронної пошти працівниками охоплюється BDSG. Як ми вже з'ясували, Розділ 32 BDSG дозволяє обробку даних, якщо це необхідно та пропорційно.

Хоча для роботодавців надзвичайно важливо знати, чи застосовується TKG, це спірно та досить невизначено. Вирішальне питання полягає в тому, чи роботодавець є *Diensteanbieter* (постачальником послуг) у значенні TKG чи ні. Якщо він/вона є постачальником послуг, на нього/неї поширюється більшість правил TKG. Вирішальне правило містить розділ 3 № 6 TKG. Відповідно до цього припису виконавцем послуг є особа, яка професійно надає телекомунікаційні послуги або допомагає в наданні таких послуг.

У минулому в Німеччині панувала думка, що роботодавець був постачальником послуг, якщо він/вона дозволяв своїм працівникам використовувати його/її телекомунікаційні засоби в приватних цілях (наприклад, дзвінок додому або використання приватних служб веб-пошти), навіть якщо були певні обмеження щодо використання цих засобів у особистих цілях. І у той же час, роботодавець не вважався надавачем послуг, якщо він/вона забороняв приватне використання таких засобів. Ця

диференціація є все ще досить поширеною в ФРН. Фактично це означає, що стеження за Інтернетом та електронною поштою можливо (окрім технічних чи платіжних причин), якщо роботодавець дозволяє своїм працівникам використовувати засоби телекомунікацій в особистих цілях. Проте протягом останніх кількох років кілька *Landesarbeitsgerichte* (Вищий Трудовий суд, LAG) стверджував, що роботодавець не є постачальником послуг, навіть якщо він дозволяє своїм працівникам користуватися телекомунікаційними засобами в приватному порядку [39; 45; 38]. Головний аргумент для цієї думки є те, що TKG керує конкуренцією на ринку телекомунікаційних послуг. Але роботодавець не конкурує з телекомунікаціями компаній, якщо він дозволяє своїм працівникам використовувати телекомунікаційні засоби для приватних цілей. У цьому контексті він не діє заради прибутку. Роботодавець просто хоче створити якісь зручності для своїх співробітників і бажає сприяти балансу між роботою та життям. Тому він не повинен дотримуватися у цих ситуаціях TKG.

Ця думка швидко набирає популярності, цілком імовірно, що вона стане переважаючою у найближчому майбутньому. Сутність полягатиме в тому, що стеження за використанням Інтернету та електронної пошти має бути пропорційним відповідно до розділу 32 BDSG. Хоча правова ситуація невизначена і кожну обробку потрібно буде оцінювати в світлі окремого випадку, але можна визначити певні принципи: дані, які є явно приватними (наприклад, запрошення на вечерю), не повинні підлягати обробці. Файли журналу, що містять лише технологічні дані (наприклад, час, коли електронний лист було надіслано, обсяг переданих даних) можна обробити, але не файли з реальним вмістом (наприклад, текст або зображення).

Відтак, обсяг даних, що обробляються, необхідно якомога зменшити. Прозора обробка є правилом, таємна обробка є абсолютним винятком. Для підтвердження злочинної поведінки працівника може проводитися таємна обробка, але навіть тоді вона має ретельно розглядатися і може бути лише крайнім заходом.

Корпоративним групам регулярно потрібно передавати особисті дані співробітників між собою. Між членами групи часто обробляються дані

співробітників, особливо керівником групи, принаймні для певних цілей (наприклад, табелювання, нарахування заробітної плати). Крім того, певні служби всієї групи можуть бути об’єднані в одну (наприклад, ІТ-послуги). За таких обставин дані часто необхідно передати від учасника групи А до учасника групи Б. Ця передача є обробкою даних, які потребують обґрунтування. Однак справи йдуть складніше, якщо член групи А та член групи В не розташовані в одному місці країни.

До тих пір, поки член групи А і член групи В знаходяться в межах ЄС, передачу персональних даних слід розглядати як передачу даних у межах ФРН. Однак згідно з Директивою 95/46/ЄС застосовуються спеціальні правила, якщо учасник групи А знаходиться в країні ЄС, а учасник групи В – у країні, що не входить до ЄС (третя країна).

Згідно зі ст. 25 Директиви 95/46/ЄС, держави-члени забезпечують, щоб передача персональних даних до третьої країни може відбутися лише за умови, що йдеться про третю країну, яка забезпечує належний рівень захисту. Адекватність наданого рівня захисту третьою країною оцінюється в світлі всіх обставин передачі даних. Європейська комісія може виявити, що третя країна забезпечує відповідний рівень захисту. Рішення Європейської комісії з цього питання є обов’язковим для виконання держав-членів.

Треті країни, що мають належний рівень захисту з точки зору Європейської комісії в даний час до їх складу входять: Андорра, Аргентина, Австралія, Канада, Швейцарія, Фарерські острови, Гернсі, Ізраїль, острів Мен, Джерсі, Нова Зеландія та Східна Республіка Уругвай [3].

Стаття 26 Директиви 95/46/ЄС дозволяє відступи від принципу, викладеного в ст. 25 Директива 95/46/ЄС. Відступи можуть застосовуватися, якщо:

– суб'єкт даних дав однозначну згоду на запропоновану передачу;

– передача необхідна для виконання договору між даними суб'єкта та контролера або здійснення переддоговірних заходів взятих у відповідь на запит суб'єкта даних;

– передача необхідна для укладення або виконання договору укладеного в інтересах суб’єкта даних між контролером і третьою особою;

– передача необхідна або вимагається законом з важливих суспільних інтересів, або для встановлення, здійснення чи захисту правових вимог;

– передача необхідна для захисту життєво важливих інтересів суб’єкта даних;

– перенесення здійснюється з реєстру, який відповідно до законів чи нормативних актів є призначений для надання інформації громадськості та відкритий для консультацій або для громадськості в цілому, або будь-якою особою, яка може продемонструвати законність інтересу, у тій мірі, в якій умови, встановлені законом для консультації виконуються в конкретному випадку.

Однак застосовність цих відступів необхідно оцінювати в світлі кожного окремого випадку. Таким чином, вони не є надійною основою для передачі даних в міжнародних групах компаній. Якщо третя країна не має належного рівня захисту та жодного з наведених відступів не може бути застосовано, то член групи А може, тим не менш, передавати дані члену групи В, який знаходиться в третій країні, за умови, що член групи А наводить належні гарантії щодо захисту даних щодо приватного життя та основних прав та свобод особи.

Існують різні способи забезпечити такі гарантії:

– стандартні договірні положення. Європейська комісія опублікувала три комплекти типових контрактів, які регулюють передачу персональних даних між сторонами, розташованих в державах-членах і третій країні [66]. Ці стандартні договірні положення повинні бути погоджені сторонами без поправок для створення відповідних гарантій визначених у ст. 26 Директиви 95/46/ЄС. Стандартні договірні положення є бажаними, якщо потрібно здійснити обмін даними не більше ніж між двома учасниками групи. Однак даними більше не можна буде керувати, якщо передача відбувається між різними членами групи, оскільки це вимагатиме складної мережі контрактів. У такій ситуації діють обов’язкові корпоративні правила:

– сторони можуть домовитися за окремими умовами договору, скоригованими до потреб сторін. Однак, ці пункти повинні бути прийняті органами захисту даних. Навіть якщо вони бажають дати свою згоду, індивідуальними договірні положення є дуже непрактичним інструментом;

– обов'язкові корпоративні правила є альтернативою стандартним договірним положенням у випадках, коли більше двох членів групи потрібно передавати дані один одному дані [66]. Щодо організації такого корпоративного правила, то надзвичайно важливо, щоб вони були складені юридично обов’язковим способом, що однаково є обов’язковим для всіх компаній групи, і що ця домовленість реалізується у відповідній компанії у формі інструкцій відповідного роботодавця щодо всіх працівників.

Спеціальні правила застосовуються щодо Сполучених Штатів Америки. Так, США вважаються однією з держав без належного рівня захисту даних з боку ЄС. Хоча ще у 2000 році ЄС уклав угоду зі США про так звану «безпечну гавань» (Угода про безпечну гавань). Відповідно до договору належний рівень захисту персональних даних передбачається в компаніях, які стверджують, що вони поважають принципи, викладені в угоді та, які перевіряють свою практику передачі персональних даних відповідним чином. Теоретично виконання цих зобов'язань контролюється незалежними аудиторськими фірмами, а також Федеральною торговою комісією Міністерства торгівлі США, яка має право карати за порушення шляхом накладення значних штрафів. Однак останні дослідження показали, що принципи «гавані» на практиці широко нехтуються [36].

Ще у 2012 році Європейська комісія запропонувала серйозну реформу законодавства ЄС щодо захисту персональних даних. Наріжний камінь реформ, започаткованих Комісією пропонував «Загальний регламент захисту даних» [56]. Ця пропозиція чітко стосується обробки даних у контексті працевлаштування вперше на європейському рівні. Однак це скоріше ненормативний акт, оскільки ст. 82 Закону встановлює так зване початкове положення для держав-членів, зокрема встановлено, що держави-члени можуть прийняти спеціальні правила регулювання обробки персональних

даних працівників у контексті працевлаштування, зокрема для цілей найму, виконання трудового договору, включаючи виконання зобов'язань, встановлених законом або колективними договорами, управління, планування та організації праці, охорони праці та безпеки життєдіяльності, а також для цілей здійснення та користування, на індивідуальній чи колективній основі, права та пільги, пов’язані з працевлаштуванням, а також з метою припинення трудових відносин.

Що насправді мається на увазі під цим пунктом, залишається незрозумілим: чи можуть держави-члени суттєво відступають від стандарту регулювання? Редакція ст. 82 свідчить про інше. Але якщо це так, то яка користь на практиці від ст. 82? Один з головних недоліків поточної бази – це менше матеріального права, а баланс інтересів дозволяє адекватні і, перш за все, гнучкі рішення, але скоріше його розрізнене впровадження і застосування по всьому Союзу.

Конституційна скарга [42] стосувалася повноважень *Bundesnachrichtendienst* (Федеральна розвідувальна служба) для моніторингу, запису та оцінки телекомунікаційного трафіку та передачі отриманих даних іншим державним установам. За оскаржуваним юридичним положенням, моніторинг був допустимий у двох формах: моніторинг окремих осіб і стратегічне спостереження. *С*каржники поставили під сумнів, чи сумісні ці правила зі ст. 10 Основного Закону, який гарантує конфіденційність листування, пошти та телекомунікацій як фундаментального права.

Суд постановив, що ст. 10 Основного Закону не тільки забезпечує захист від взяття до відома держави телекомунікаційних контактів, але й захист процедур, за допомогою яких інформація та дані обробляються відповідно до дозволених дій взяття до відома телекомунікаційних контактів, і це поширюється на використання отриманого знання. Крім того, ст. 10 Основного закону зобов’язує Федеральну розвідку до вжиття запобіжних заходів проти небезпек, які є результатом збору та використання персональних даних. До цих запобіжних заходів належить, зокрема те, що використання отриманих знань має бути прив’язане до мети, яка виправдовує збір даних.

Також Суд вирішив, що до компетенції Федеральної Розвідувальної служби входить моніторинг, запис та оцінка телекомунікаційного трафіку для своєчасного визнання зазначеного серйозним Загрозам ФРН з-за кордону та для інформації Федерального уряду, а тому відповідає ст. 10 Основного закону. Передача персональних даних, отриманих Федеральною розвідувальною службою від моніторингу телекомунікацій для власних цілей, іншим державним органам відповідно до ст. 10 Основного Закону; однак він повинен відповідати наступним передумовам: (1) дані необхідні для досягнення цілей агентства-одержувача; (2) специфічні вимоги, що висуваються до зміни мети, виконуються; та (3) законодавчі пороги для передачі, що відповідає принципу пропорційності.

Інший приклад, справа Федерального трудового суду ФРН щодо обшуку камери схову для працівників [13]. Так, роботодавець займався продажем товарів. Позивачка була однією із його працівників. Працівницю роботодавець запідозрив у крадіжці білизни з ринку. Без дозволу працівниці роботодавець таємно відкрив камеру схову, якою користувалася працівниця для зберігання особистих речей, а в шафці знайшов жіночу білизну.

Суд постановив, що відкриття та обшук камери схову було незаконним відповідно до розділу 32 BDSG. Мета (боротьба з крадіжками) була законною, але таємне відкриття шафки порушувало принцип пропорційності, оскільки це не було необхідним для досягнення цієї законної мети. Було б достатньо, якщо роботодавець відкрив камеру схову після повідомлення та в присутності працівниці. BAG також постановив, що інформація, отримана в результаті цього незаконного обшуку не може бути використана як доказ у подальшій справі про захист від звільнення.

У судовій практиці ФРН є багато справ Федерального трудового суду щодо захисту даних під час відеоспостереження. Законодавець кодифікував цю судову практику [16]. Багато випадків стосувалися встановлення систем відеоспостереження в супермаркетах [14] або магазинах [15; 16].

Суд постановив, що обґрунтовуючи перевірку пропорційності в усіх окремих випадках, що перш ніж встановити пристрої відеоспостереження,

повинні бути достатні підстави для підозри (наприклад, нерозкрита крадіжка), які виправдовують стеження. Якесь розпливчасте припущення або загальна підозрілість щодо всіх співробітників є недостатньою. Відео стеження повинно проводитися відкрито, а не таємно. Таємне спостереження прийнятним є *ultima ratio*, щоб захистити роботодавця від серйозних порушень його інтересів (наприклад, крадіжка чи інша злочинна діяльність). Якщо ці умови виконуються, інформація зібрана за допомогою методів таємного спостереження може бути підставою для звільнення працівника. У цьому контексті розділ 6b (2) BDSG, який передбачає використання попередження як ознаки, слід тлумачити як процесуальне положення, яке не перешкоджає використанню такої інформації в позовах.

Ще одним прикладом є справа щодо обробки персональних даних на основі угоди між роботодавцем і виробничою радою.

Відповідно до розділу 77 *Betriebsverfassungsgesetz* (Закон про виробничі ради, BetrVG), роботодавець і виробнича рада є представницьким органом цехового рівня, який обирається працівниками, які можуть укласти *Betriebsvereinbarung* (робочу угоду), обов'язкову для роботодавця та для всіх працівників відповідного підприємства. Ця угода про виконання робіт є іншим правовим положенням у значенні розділу 4 (1) BDSG та тому може виправдати обробку даних.

У справі 1986 року [17] BAG мав вирішити, чи уклали сторони угоду про виконання робіт, якою було дозволено узгодити терміни та умови обробки персональних даних, які були невигідним для працівників у порівнянні з правилами BDSG.

У цьому випадку трудовий договір регулював використання телефонів роботодавця для особистих цілях співробітників. Співробітникам було дозволено користуватися телефонами для приватних цілей. Однак договір надавав роботодавцю право опрацювання набраних номерів телефонів, а також час і тривалість з'єднань, так що працівників зміг розрахувати суми, які заборгували працівники, і боротися з шахрайством.

Пізніше робоча рада стверджувала, що угода була незаконною, оскільки вона, по-перше, порушувала основні права працівників, по-друге, суперечило правилам BDSG.

Суд постановив, що зміст угоди про виконання робіт не обмежувався BDSG. Якщо договір був «іншим правовим положенням» у розумінні розділу 4 (1) BDSG, згідно з яким судді не обмежуються обґрунтуванням норм цього акта. Натомість можна було узгодити умови обробки даних, які були невигідними для працівників порівняно з правилами BDSG. Обмеження свободи сторони, які погоджуються щодо таких умов, повинні випливати з Конституції і тільки підконституційний обов'язковий закон (не включаючи BDSG). Хоч суд підтримав цю позицію в рішенні 1995 року, вона викликає серйозні суперечки в сучасних дебатах [37].

Однак у 2013 році BAG знову підтримав попереднє рішення та неодноразово наголошував, що договір про виконання робіт був «іншим правовим положенням» у значенні розділу 4 (1) BDSG був дійсним та пропорційним та сумісним лише з основними правами [21].

У Конституції Франції не має згадки про захист персональних даних, інформації та особисту конфіденційність працівників. Однак *Conseil constitutionnel* визнав право на недоторканність приватного життя в 1996 [28] та з того часу почалися розробки нормативної бази про захист персональної інформації [29]. В останні роки обговорюється можливість внести зміни до Конституції, щоб чітко гарантувати право захист персональних даних. Проте вважають, що ця зміна не повинна бути пріоритетною [60], позаяк гарантії, що випливають із практики конституційного суду та з міжнародних документів вважаються достатніми. Дійсно, кілька міжнародних інструментів захищають конфіденційність та особисту інформацію. Найважливішими є ті, що розроблені Радою Європи та ЄС [74].

Французьке законодавство запровадило два механізми захисту особистої інформації та конфіденційності працівників.

Ще Закон № 78-17 від 6 січня 1978 р. про інформаційні технології, бази даних [59] мав би вирішити більшість проблем, що виникли в результаті

використання комп'ютерів. Однак все ж це було переважно захисне право, яке першочергово спрямоване було на запобігання виникненню витоку інформації на рівні держави. А ось зростаюче використання нових інформаційних технологій у трудових відносинах, ані розвиток інформаційного суспільства, не очікувався тоді. Тим не менш, зміни міжнародного та європейського законодавства спричинили адаптацію цього закону до реалій, і хоча Закон було розроблено для використання в державному секторі, все ж його положення досить адаптовані до приватного сектору і трудових відносин.

А ось Закон № 92-1446 від 31 грудня 1992 року мав іншу мету. Лише п’ять статей цього акту присвячені правам і свободам працівників. Між тим ці статті мали головну мету. Їх введенню в дію передувала важлива робота Комісії [46], спрямована на захист конфіденційності та особистого життя працівників від влади роботодавця [30; 7]. Ці 5 статей кодифіковано в *Code du travail (Labor Code)* і, що символічно, вони були розміщені одними з перших у новому Кодексі 2008 року.

Закон № 78-17 від 6 січня 1978 р. та Закон № 92-1446 від 31 грудня 1992 р. мають різні сфери застосування. Перший Закон застосовується, якщо будь-хто обробляє особисту інформацію працівника, чи то роботодавець, чи хтось інший. Другий Закон застосовується якщо дії роботодавця створюють небезпеку для прав і свобод працівника. Крім того, обидва акти впроваджують різні механізми захисту особистої інформації та конфіденційності працівників. Тому на практиці перевіряється відповідність щодо обох актів. Коли роботодавець використовує технологію для збору або збереження особистої інформації працівників, то варто враховувати кілька умов, перерахованих у Законі 1978 року, а також необхідно виконати деякі формальності, як-от: повідомлення про обробку персональних даних незалежного адміністративного органу або отримання згоди. Якщо ці вимоги не дотримані, то за порушення передбачена кримінальна відповідальність. Однак на практиці такі санкції застосовуються вкрай рідко [22]. Адже вважається, що найбільш ефективним засобом захисту є дотримання приписів

Закону, а також заборона використовувати дані, зібрані незаконним шляхом, як доказ у дисциплінарній відповідальності чи судовому процесі.

Французький орган захисту даних, який називається *CNIL (French data protection authority)*, є незалежним адміністративним органом, який відіграє важливу роль у забезпеченні дотриманні закону. CNIL має дві місії:

1) його члени та посадові особи контролюють, чи роботодавець, який обробляє персональні дані працівників, дотримується законодавства. Тому робітник, який стикається з труднощами щодо своїх персональних даних, може подати свою справу до CNIL. Однак у цьому випадку CNIL має обмежені можливості: у разі незначного порушення комісія може надіслати офіційні повідомлення та накладати фінансові санкції, але в разі значного порушення це підпадає під юрисдикцію прокурора і кримінальних судів;

2) поради компаніям, працівникам і громадянам. CNIL сприяє регулюванню використання нових технологій. Навіть якщо ці міркування не є обов'язковими, це «м'яке право» має суттєвий вплив на юридичну практику, особливо тому, що члени CNIL можуть висловити свою думку відразу без необхідності чекати судового розгляду. Тобто CNIL сьогодні є радше організацією, яка розробляє доктрину захисту персональної інформації та конфіденційності, ніж орган, який контролює поведінку роботодавця у цій царині.

Всередині фірми дії CNIL ретранслюються захистом персональних даних спеціально створеним структурним підрозділом (посадовою особою) – *Correspondant Informatique et Liberté (CIL).* Варто зауважити, що Закон 1978 року не надає значної ролі традиційним системам стримувань і противаг: профспілки та виборні представники персоналу ігноруються, а тому створення нового підрозділу всередині фірми може бути поставлено під сумнів [58].

CIL має контролювати поведінку роботодавця, але для того, щоб виконати це завдання, йому потрібно мати багато якостей: володіння комп'ютером, хороші знання законодавства та організації фірми, а також незалежність від свого керівника. Такий набір якостей важко знайти. Крім того, законодавець не надав CIL статусу, подібного до статусу

представницьких органів працівників. У більшості випадків CIL є співробітником фірми та не має правового захисту від роботодавця. Тож на практиці CIL вміє пропагувати доктрину CNIL, а не контролювати дії роботодавця.

Захист персональних даних працівників, запроваджений Законом 1992 року, актуальний лише тоді, коли діють є небезпека для свобод працівників. Наприклад, коли роботодавець планує запровадити систему охоронного відеонагляду (CCTV) або коли роботодавець приймає індивідуальне рішення про конфіденційність співробітника. У цій ситуації роботодавець повинен продемонструвати, що втручання в права і свободи працівника виправдані законною метою і пропорційні їй [44]. У багатьох випадках він також повинен виконувати обов'язок розкриття [44].

Найважливішими засобами захисту є визнання рішення роботодавця недійсним та відшкодування шкоди, а також неможливість для роботодавця неправомірного використання інформації, зібраної як докази. До роботодавця також можуть бути застосовані кримінальні покарання [31], але ці санкції на практиці застосовуються рідко.

Засоби примусового виконання Закону № 92-1446 від 31 грудня 1992 року є більш традиційними, ніж Закон № 78-17 від 6 січня 1978 р. Якщо Закон порушується, то працівники могли звернутися до цивільного судді – у разі індивідуального рішення або якщо працівник постраждав від шкоди його/її персональним даним – або адміністративному судді – у разі рішення щодо всіх працівників. Постанови двох вищих цивільних та адміністративних судів, *Cour de cassation ma Conseil d Etat*, сприють визначенню значення цього законодавства щодо розробки нових технологій та використання нових методів управління.

У Франції безпосередньо на місці роботи представник, обраний іншими працівниками, називається *Délégué du personne*l (DP) та відіграє найважливішу роль у захисті персональних даних працівників. DP не має права вето рішення роботодавця, але може запитати роботодавця про його мету та методи обробки

персональних даних працівників. Якщо DP не переконують аргументи роботодавця, він може звернутися до судді у спрощеному порядку [44].

Маючи подвійну законодавчу систему захисту персональних даних працівників, в багатьох випадках два проаналізовані вище закони застосовуються разом. У таких ситуаціях і CNIL, і суддя повинні забезпечити відповідність дій роботодавця положенням законодавства.

Вплив європейських інструментів на правовий захист працівників особистої інформації та конфіденційності зростає протягом багатьох років. Директива 95/46/ЄС від 24 жовтня 1995 р. була імплементована у Франції в 2004 році. Завдяки цьому посилено репресивні повноваження CNIL і створено CIL. Закон про інформаційні технології, бази даних наразі слід тлумачити відповідно до Директиви. З іншого боку, правила, визначені Директивою є більш ефективними, оскільки реалізація її положень здійснюється згідно з контролем Комісії та Європейського суду. Це також полегшує співробітництво між наглядовими органами в межах ЄС. З огляду на французьку систему, пропозиції Комісії могли б змінити місії наглядових органів, які мали б у майбутньому більше повноважень щодо припинення правопорушень. Така еволюція закладала б значні зміни в організації та діяльності CNIL.

Для досягнення балансу між інтересами роботодавця і працівників використовуються різні методи. Якщо в інших країнах, основоположну роль відіграє принцип пропорційності, то у Франції розвиваються й інші підходи. (A) Баланс досягається, коли роботодавець прагне отримати персональну інформацію працівника. (B) Коли роботодавець хоче прийняти рішення, пов'язане з особистим життям працівника.

A. Збір особистої інформації співробітників.

Коли роботодавець прагне збирати персональну інформацію працівників, керівним принципом є законність – дії роботодавця повинні мати законну мету

втручання у свободу працівника, що має бути пропорційним цій меті.

Те ж саме викладено і у ст. L. 1121-1 Трудового кодексу Франції, зокрема, що ніхто не може обмежувати особисті права, ані індивідуальні, ані колективні свободи, якщо це обмеження не виправдане природою роботи, яка має бути виконана та пропорційна переслідуваній меті. А ст. L. 1222-2, al 2 Трудового кодексу Франції встановлює, що інформація, яку запитують у працівника, повинна мати безпосередній і необхідний зв'язок з оцінкою його професійної майстерності. Крім того, ст. 6 Закону про інформаційні технології, бази даних і громадянські свободи передбачає, що персональні дані повинні бути отримані для визначених, явних і законних цілей, повинні бути адекватними, відповідними та не надмірними щодо цілей, для яких вони призначені, отримані та їх подальша обробка. Отже, рішення роботодавця має бути законним і пропорційним.

Легітимність цілей зазвичай не важко довести. Роботодавець може легко продемонструвати, що його/її дії можуть захистити фірму від крадіжок або можуть покращити продуктивність компанії. Отже, ключова концепція для досягнення балансу між інтересами роботодавця та працівників принцип пропорційності. Пропорційність втручання у свободу працівника оцінюється в кожному конкретному випадку [57, с. 31-38].

**Висновки до розділу 1**

За результатами вивчення теоретичних засад захисту персональних даних працівників, ми дійшли таких висновків.

1. Захист персональних даних працівника є елементом трудових правовідносин, а також з метою забезпечення їх одноманітного правового режиму, захист персональних даних працівника слід розглядати як самостійний інститут трудового права. Адже суспільні відносини, пов'язані із захистом персональних даних працівника, є окремими видами правовідносин у сфері праці, які можуть як передувати (надання інформації в ході працевлаштування у певного роботодавця), супроводжувати (приміром,

ухвалення рішення про просуванні працівника по службі), так і випливати з трудових правовідносин (приміром, розголошення комерційної таємниці), специфіка яких пов'язана з ключовими суб'єктами трудового права – працівниками та роботодавцями.

2. Інформація про заробітну плату, премії, матеріальну допомогу, будь-які інші виплати з державного чи місцевого бюджету працівнику державного органу або органу місцевого самоврядування не є конфіденційною, не може бути обмежена в доступі та підлягає наданню на запит.

3. Персональні дані працівника – це інформація, яка стосується загальних даних про особу працівника та/або кандидата на посаду, професійної кваліфікації працівника/кандидата на посаду, ділових, професійних якостей, а також інформація щодо спеціальних вимог, які можуть встановлюватися законодавством до працівників/кандидатів на посаду у зв'язку з характером їх роботи (приміром, заповнення декларації про доходи, проходження спеціальної перевірки тощо). Тобто персональні дані працівника мають забезпечувати ідентифікацію його/її не тільки і не стільки як людину, а насамперед як працівника. Це означає, що персональні дані працівника та претендента на посаду – це, в першу чергу, інформація, що стосується професійної кваліфікації, ділових, професійних якостей та відповідності працівника та претендента на посаду вимогам, які можуть бути до нього пред'явлені у зв'язку з характером роботи.

4. Класифікація персональних даних працівника, в аспекті їх збору, обробки та правового режиму використання має провадитися на такі групи:

а) загальні «анкетні» персональні дані (відомості про прізвище, ім’я, по батькові, дата та місце народження, паспортні дані, відомості про освіту, про професійні навички, відомості про «історію» трудової діяльності тощо);

б) спеціальні персональні дані: расова, національна приналежність, політичні погляди, релігійні чи філософські переконання, стан здоров'я, приватне життя. Збір та обробка цих персональних даних має бути заборонена для роботодавця;

в) персональні дані обмеженого доступу, до яких слід віднести відомості про усиновлення, судимість, участі у кримінальному судочинстві як підозрюваного, наданої чи прийнятої фінансової допомоги, чи послуг, декларація про доходи, результати спеціальної перевірки тощо;

г) біометричні персональні дані – відомості, що містять характеристики фізіологічних та біологічних особливостей людини, що дають можливість встановлення її особистості. Ці дані є «чутливими даними» і мають особливий правовий режим захисту. Для їх обробки роботодавцем потрібне спеціальне погодження Уповноваженим ВРУ.

5. Роботодавець не має права знищувати документи з персональними даними працівника (особову картку П-2 чи документи особової справи). У працівника як суб'єкта персональних даних є право вмотивованої вимоги знищити персональні дані. Однак, право виникає лише тоді, коли дані обробляються незаконно чи є недостовірними.

6. Специфіка захисту персональних даних осіб, які здійснюють свою професійну діяльність на підставі трудового договору, проявляється, перш за все, в тому, що основні вимоги щодо обробки персональних даних працівника встановлюються нормами законодавства, а порядок здійснення окремих операцій з персональними даними працівника (збір, зберігання, використання, поширення) може деталізуватися у локальних правових актах. Обов'язок не розголошувати персональні дані також може бути передбачений законами та підзаконними актами для окремих категорій осіб, наприклад, для державних службовців.

7. Виокремлено чотири кроки, щоб захистити персональні дані працівника на підприємстві:

а) визначити технічні та організаційні заходи, які треба вжити;

б) призначити відповідального за обробку і захист персональних даних. Якщо роботодавець — орган влади, ОМС чи підприємство, що обробляє чутливі персональні дані, призначайте відповідального обов'язкового. В інших випадках — за рішенням керівника підприємства;

в) розробити Положення про порядок обробки та захисту персональних даних;

г) отримати зобов’язання про нерозголошення персональних даних від працівників, які стикаються під час роботи з персональними даними інших осіб. Зареєструвати отримані зобов’язання в Журналі реєстрації зобов’язань про нерозголошення персональних даних.

# РОЗДІЛ 2
# СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ В УКРАЇНІ

## 2.1. Сучасний стан, становлення та розвиток державних механізмів забезпечення захисту персональних даних працівників

Як справедливо відзначає А. М. Чернобай, право на захист персональних даних працівника не могло бути реалізовано у радянський період. Втручання в особисте життя з боку держави, адміністрації підприємств, установ, організацій, партійних комітетів, спецслужб, різних контрольних органів носило надзвичайний характер, у зв'язку з чим питання про захист персональних даних навіть не виникало. У зв'язку з цим, обов'язковими були особові листки з обліку кадрів, характеристики, анкети та інші документи, які треба було заповнити або подати при прийнятті на роботу, виїзді з країни у закордонне відродження або туристичну поїздку тощо. В особовому листку з обліку кадрів треба було відповісти на велику кількість питань, які не мали відношення до професійних якостей працівника, а стосувалися обставин його особистого життя: про соціальне походження батьків, партійності (якою організацією був прийнятий у члени КПРС, чи мав партійні стягнення, чи перебував раніше в партії та причина виключення або вибування, чи брав участь в антипартійних угрупуваннях (яких, коли) і чи мав коливання від проведення лінії партії), про перебування за кордоном (число, рік, місяць, в якій країні, мета перебування), на тимчасово окупованій території під час Великої Вітчизняної війни, наявність родичів у зарубіжних країнах, виконувану роботу з початку – трудової діяльності, сімейний стан з перерахуванням складу родини та ін. Ніякими резюме для кадрових служб із перерахуванням ділових персональних даних працівника замінити особові листки з обліку кадрів і анкети тоді було не можна.

За часів незалежності України в останнє десятиріччя XXI століття становище докорінно змінилося, відбулися значні перетворення в усіх сферах діяльності, пов'язані з переходом до ринкової економіки, побудови

демократичної, соціальної, правової держави, визнанням загальнолюдських цінностей, принципів і норм міжнародного права, захистом прав і свобод людини та громадянина. У цей період були прийняті закони «Про інформацію» від 2 жовтня 1992 року, «Про захист інформації в автоматизованих системах» від 5 липня 1994 року (діє в новій редакції Закону України від 31 травня 2005 року з новою назвою «Про захист інформації в інформаційно-телекомунікаційних системах») [136], які за відсутності спеціальних правових норм певною мірою регулюють відносини щодо захисту персональних даних працівника. У цей час в Україні діє понад два десятки законодавчих актів, які тією чи іншою мірою регулюють відносини, пов'язані зі збором, використанням і передачею персональних даних [175, с. 7-8].

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 [101]. Положення цієї статті було роз’яснено в рішенні Конституційного суду України від 20 січня 2012 року 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 [158]. КСУ дійшов висновку, що 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, відомості про її майновий стан та інші персональні дані. Таким чином, КСУ вважає, що перелік даних про особу, які визнаються як конфіденційна інформація, не є вичерпним.

Підсумувавши, КСУ дійшов висновку, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров’я, матеріальний стан, адреса, дата і місце

народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [158].

Варто зауважити, що незважаючи на наявність конституційної норми щодо захисту конфіденційного інформації, фактично захист персональних даних (далі – ЗПД) як такий запроваджено в Україні лише з 01.01.2011 р. Наразі правові відносини, пов'язані із захистом і обробкою персональних даних, регулює Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI (далі – Закон № 2297) [137]. Наголосимо, що первинна редакція Закону № 2297 [137] не відповідала повною мірою міжнародним актам. Однак у 2012 році до Закону № 2297 [137] внесли істотні зміни, зокрема, ввели законодавчі підстави для роботи з персональними даними контрагентів, а у 2014 році – підстави для роботи з персональними даними працівників. Саме тоді спростили процедуру документування роботи з персональними даними, яка в первинній редакції була занадто бюрократизованою.

Контроль за дотриманням законодавства у сфері захисту персональних даних наразі покладено на Уповноваженого Верховної Ради України з прав людини (омбудсмена). А контрольні функції реалізує спеціально створений в Секретаріаті Уповноваженого Департамент з питань захисту персональних даних. Однак до 2014 року контролюючим органом у цій сфері була Державна служба з питань захисту персональних даних [146], але Службу ліквідували [145; 122].

Поряд із Законом № 2297 [137] захист персональних даних регламентують такі підзаконні акти:

– Типовий порядок обробки персональних даних (далі — Типовий порядок обробки ПД);

– Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних (далі – Порядок контролю);

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

Усі ці порядки затверджені наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 [128].

Окрім цього, є суб'єкти господарювання, що на додачу до вимог Закону № 2297 мають додержувати й положень європейського Загального регламенту про захист даних (GDPR) [63]. Наприклад, дочірні підприємства міжнародних компаній в Україні; компанії, що постачають товари чи надають послуги фізичним особам в ЄС, зокрема безоплатно.

Перший етап становлення формування правового регулювання використання персональних даних розпочався з часу прийняття у першій редакції Закону України «Про інформацію» від 2 жовтня 1992 р. [139], де у ст. 28 (у тій редакції) зазначалось, що за режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. А ось ст. 30 визначала, що інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну і таємну. Тоді конфіденціальна інформація визначалась як відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. За тогочасними нормами громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного,

ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденціальної, та встановлюють для неї систему (способи) захисту. Виняток становила інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено ВРУ за поданням КМУ (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої становило загрозу життю і здоров'ю людей. Проте про який виняток йшла мова: про віднесення цієї інформації до таємної чи до відкритої – законодавець не уточняв. Це створювало певну невизначеність щодо правового режиму такої інформації.

До таємної інформації на той період належала інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснювався як і зараз відповідно до закону про цю інформацію.

У Законі України «Про інформацію» [139] законодавець не визначав режиму доступу до інформації про особу як до конфіденціальної чи до таємної інформації. Проте у ст. 32 Конституції України [101] згадується термін «конфіденційна інформація про особу». Водночас інші положення цієї статті Конституції України знайшли відображення у Законі України «Про інформацію» [139], де було відокремлено окремі статті, що визначали зміст та порядок використання інформації про особу: статті 23 та 31. Так, відповідно до цих статей інформація про особу – це сукупність документованих або публічно оголошених відомостей про особу. Аналіз зазначених статей (у їх тодішній редакції) дозволив виокремити наступні ознаки відомостей, що мають правовий статус персональних даних: 1) за змістом це відомості про національність, освіту, сімейний стан, релігійність, стан здоров'я, а також адресу, дата і місце народження (основні персональні дані); 2) джерелами документованої інформації про особу є видані на її ім'я документи, підписані

нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень; 3) умовою збирання відомостей про особу є її попередня згода, за винятком випадків, передбачених законом. Основні правила користування персональними даними, що утворюють її правовий режим визначені були також у ст. 31. Частина цих положень є реалізацією норм ст. 32 Конституції України [101].

Характеризуючи тогочасний правовий режим персональних даних як виду інформації з обмеженим доступом, необхідно зазначити, що відповідно до ст. 37 Закону України «Про інформацію» [139]: «Документи та інформація, що не підлягають наданню для ознайомлення за запитами» окремими пунктами переліковувала офіційні документи, що не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами, які містять у собі конфіденціальну інформацію та інформацію, що стосується особистого життя громадян. Таким чином, законодавець розмежовував поняття «персональні дані» та «конфіденціальна інформація».

Другий етап розпочався (умовно) 30 жовтня 1997 р. з наданням офіційного тлумачення поняття «персональні дані» Конституційним Судом України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та ст. 12 Закону України «Про прокуратуру» (справа К. Г. Устименка). У цьому роз’ясненні вперше на офіційному рівні було визнано, що вітчизняним законодавством не повністю визначено режим збирання, зберігання, використання та поширення інформації, зокрема щодо психічного стану людини, її примусового огляду та лікування, не створено процедуру захисту прав особи від протизаконного втручання в її особисте життя психіатричних служб. Закон України «Про інформацію» закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особисто. Механізм реалізації зазначеного права належним чином не визначений. Відсутнє й регулювання використання конфіденційних даних у сфері психіатрії [159]. Водночас КСУ назвав перелічені у Законі України «Про інформацію» [139] відомості про особу конфіденційною інформацією, і відніс

до неї дані про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані), таким чином, розширивши зміст персональних даних за рахунок відомостей про майновий стан.

Третій етап включає внесення суттєвих змін до Закону України «Про інформацію» [139] (в редакції від 09.06.2004 р.), до якого були внесені зміни відповідно до Закону України «Про внесення змін до деяких законодавчих актів України» від 11 травня 2004 р. № 1703-IV [124], у зв’язку із якими конструкція «конфіденціальна інформація» було замінено на «конфіденційна інформація». Водночас ст. 30 після частини другої доповнили частинами третьою та четвертою такого змісту: «Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної. Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України.

Також було визначено перелік відомостей, які не могли бути віднесені до конфіденційної інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності» Стаття 37 Закону України «Про інформацію» [139]: «Документи та інформація, що не підлягають наданню для ознайомлення за запитами» (в редакції від 09.06.2004 р.) окремими пунктами розділяє офіційні документи, які містять у собі вже конфіденційну інформацію та інформацію, що стосується особистого життя громадян.

Четвертий етап – прийняття Закону України «Про захист персональних даних» [137], створення відповідної служби і прийняття значної кількості нормативно-правових актів.

П’ятий етап – передання всіх повноважень по захисту персональних даних до Уповноваженого ВРУ з прав людини.

Порядок здійснення та забезпечення права кожного на доступ до інформації, що перебуває у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, та інформації, що становить суспільний інтерес, визначається Законом України «Про доступ до публічної інформації» [125]. Зазначений Закон покликаний забезпечувати прозорість і відкритість суб'єктів владних повноважень й створювати механізми реалізації права кожного на доступ до публічної інформації, якою є відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка міститься у володінні суб'єктів владних повноважень чи інших розпорядників публічної інформації, визначених вищезгаданим Законом. Водночас у процесі діяльності державних органів накопичується не тільки відкрита інформація, але й інформація з обмеженим доступом, що підтверджується змістом ч. 2 ст. 1 Закону України «Про доступ до публічної інформації» [125].

Конституція України у ст. 32 забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту й прав людини [101]. Принцип обов'язковості отримання згоди особи під час використання конфіденційної інформації про неї відображено у ст. 6 Закону України «Про захист персональних даних» [137], а винятки з цього правила визначено у ст. 7 зазначеного Закону [137].

Аналогічний підхід під час реалізації положень ст. 32 Конституції України повинен бути застосований і при удосконаленні правових режимів інших видів конфіденційної інформації, що визначені спеціальними нормативно-правовими актами. Згода на розголошення відомостей про особисте життя громадян, отриманих органами державної влади та об'єднаннями громадян зі звернень громадян, обов'язкова також відповідно до ст. 10 Закону України «Про звернення громадян» [138]. Цією ж нормою встановлена заборона розголошення отриманих зі звернень відомостей, що

становлять державну або іншу таємницю, яка охороняється законом без згоди особи, що звернулась.

Виходячи із наведеного, прослідковується тенденція до посилення уваги з боку законодавця щодо правового врегулювання питання захисту конфіденційної інформації фізичних осіб, проте недостатньо врегульовано це питання у випадках реалізації права на дотримання конфіденційності інформації громадських об'єднань [178, с. 85-89].

Ми вважаємо, що останнім часом у зв'язку з цифровізацією деякі зрушення щодо збору, використання та обліку персональних даних працівників все ж прослідковуються. Пригадаємо лише, що ч. 3 ст. 29 КЗпП України була доповнена приписом такого змісту: «ознайомлення працівників з наказами (розпорядженнями), повідомленнями, іншими документами роботодавця щодо їхніх прав та обов'язків допускається з використанням визначених у трудовому договорі засобів електронних комунікаційних мереж з накладенням удосконаленого електронного підпису або кваліфікованого електронного підпису». Із заглибленням процесів цифровізації цілком можливим убачається і надання працівником інформації за допомогою ІКТ із використанням електронного підпису або кваліфікованого електронного підпису.

## 2.2. Проблеми забезпечення захисту персональних даних працівників

Відповідно до приписів Закону № 2297 [137] передача відомостей про фізичну особу називається «поширення персональних даних» (ст. 14 Закону № 2297 [137]). Забезпечення захисту персональних даних працівників має відповідати технічним та організаційним вимогам.

**Технічні та організаційні засоби захисту персональних даних [118]**
Відповідно до ст. 24 Закону України № 2297:

| Аспект захисту | Технічні засоби захисту | Організаційні засоби захисту |
|---|---|---|
| Захист від несанкціонованого/незаконного доступу сторонніх осіб (з усіма наслідками) | Для персональних даних у паперовому вигляді (у т. ч. картотек):<br>– зберігання у приміщеннях (шафах, сейфах), захищених від несанкціонованого доступу;<br>– двері у приміщеннях (шафах, сейфах) повинні бути обладнані замком або контролем доступу;<br>– розмежування зон для працівників, які мають санкціонований доступ, і для інших працівників або відвідувачів.<br>Для персональних даних у складі автоматизованих систем / баз даних / інформації в електронному вигляді:<br>– застосування засобів мережевого захисту від несанкціонованого доступу;<br>– допуск працівників володільця/розпорядника лише після авторизації;<br>– блокування доступу осіб, які не пройшли процедуру ідентифікації та/або автентифікації;<br>– реєстрація результатів ідентифікації та/або автентифікації | регламентація у положенні про обробку персональних даних |

| Аспект захисту | Технічні засоби захисту | Організаційні засоби захисту |
|---|---|---|
| | працівників володільця персональних даних;<br>– реєстрація дій з обробки персональних даних | |
| Захист від розголошення службовими особами володільця або розпорядника персональних даних | – | 1) надання службовими особами зобов'язань про нерозголошення персональних даних;<br>2) фіксація відповідальності за розголошення персональних даних у посадових (робочих) інструкціях, положеннях про підрозділи, положенні про обробку персональних даних |
| Захист від випадкової втрати або зловмисного знищення службовими особами володільця чи розпорядника персональних даних | Для персональних даних у складі автоматизованих систем / баз даних / в електронному вигляді:<br>– антивірусний захист;<br>– засоби безперебійного живлення;<br>– реєстрація дій з обробки персональних даних;<br>– реєстрація результатів;<br>– перевірки цілісності засобів захисту персональних даних. | фіксація відповідальності у посадових (робочих) інструкціях, положеннях про підрозділи, положенні про обробку персональних даних |

| Аспект захисту | Технічні засоби захисту | Організаційні засоби захисту |
|---|---|---|
| | Для персональних даних у паперовому вигляді:<br>– обмеження доступу осіб;<br>– контроль за доступом до паперових носіїв | |

За загальним правилом, персональні дані можна передавати третім особам за згодою людини чи уповноваженої ним особи. Якщо згоди немає, передавати персональні дані можна за двох одночасних умов:

1) таке передання передбачено законом;

2) передання обумовлено інтересами національної безпеки, економічного добробуту та прав людини.

Для того, щоб отримати персональні дані, особа чи установа надсилає володільцю персональних даних письмовий запит (ст. 16 Закону № 2297 [137]). Вимоги до запиту про доступ до персональних даних встановлено ч. 4 ст. 16 Закону № 2297 [137], зокрема у запиті зазначають:

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;

3) підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи – заявника);

4) прізвище, ім’я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

5) відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

6) перелік персональних даних, що запитують;

7) мета та (або) правові підстави для запиту.

Наразі у той час, коли працівники знаходяться у різних куточках світу, працюють дистанційно, повсякчас виникає запитання – чи можна надати інформацію про персональні дані працівника на телефонний запит? Вважаємо, що цього робити не можна, позаяк таку інформацію слід надавати тільки за письмовими запитами та за згодою працівника, яку він/вона надав(ла), або володільцю його персональних даних, або запитувачу. Оскільки якщо передавати таку інформацію телефоном, то роботодавець ризикує, адже працівник може поскаржитися омбудсмену на те, що роботодавець незаконно поширив його/її персональні дані, а як наслідок роботодавець може отримати штраф.

Якщо все ж роботодавець отримав запит телефоном, то вважаємо, що слід пояснити запитувачу, чому не можна його задовольнити, і попросити надіслати письмовий запит, оформлений згідно з ч. 4 ст.16 Закону № 2297 [137]. Якщо роботодавець отримав письмовий запит слід перевірити, чи відповідає він вимогам ч. 4 ст. 16 Закону № 2297 [137]. Якщо запитувач не додав до запиту підтвердження згоди працівника на передання персональних даних, то роботодавець має запитати згоду самостійно, адже порядок доступу третіх осіб до персональних даних визначається умовами згоди суб'єкта персональних даних, наданої володільцю персональних даних на обробку цих даних, або відповідно до вимог закону.

Цікавим є запитання – чи надавати інформацію про персональні дані працівника на запит банку? Зазначимо, що інформацію про особу, що обробляє банк, можна умовно поділити на дві категорії:

1) інформація, яку банк має право обробляти відповідно до закону;

2) додаткові дані, які законодавство України не вимагає.

Роз'яснимо щодо кожної з категорій інформації.

Категорія 1. Банк зобов'язаний ідентифікувати особу клієнта відповідно до законодавства України (Закон України № 2121 [121]). На підставі поданих офіційних документів або засвідчених в установленому порядку їх копій банк зобов'язаний ідентифікувати клієнтів, які проводять фінансові операції. Додаткові дані для вивчення клієнта також можуть бути одержані від клієнта

або з інших джерел, якщо така інформація є публічною (відкритою) (ч. 4–13 ст. 11 Закону України від 06.12.2019 р. № 361-IX [126]).

Банк має отримати документи і відомості, що містять дані, на основі яких ідентифікується клієнт, відповідно до вищезазначених Законів та Положення про здійснення банками фінансового моніторингу [133], та інших нормативно-правових актів. Так, щоб ідентифікувати клієнта, банк отримує відомості:

– прізвище, ім’я та по батькові;

– дату народження;

– номер паспорта громадянина України або іншого документа, що посвідчує особу), дату видачі та орган, що його видав;

– місце проживання або місце перебування особи;

– реєстраційний номер облікової картки платника податків або номер паспорта громадянина України, в якому проставлено відмітку органів доходів і зборів про відмову від одержання реєстраційного номера облікової картки платника податків.

Категорія 2. Банк може отримувати додаткові відомості про клієнта, які не вимагає законодавство України. Для цього банк визначає перелік документів і відомостей та умови їх надання в договорі з клієнтом або в опитувальнику. Банк має поінформувати клієнта, що надання цих документів та відомостей не є обов’язковими згідно з вимогами законодавства, а клієнт надає їх добровільно. Отже, отримувати чи передавати такі відомості банк має тільки за згодою суб’єкта персональних даних (лист НБУ «Роз’яснення з питань здійснення ідентифікації клієнтів банків» від 11.11.2011 р. № 48-104/2256-13461 [164]).

Зауважимо, що інформація щодо того, чи працює особа в певній установі, її посади, стажу роботи, розміру зарплати тощо належить до категорії 2. Тобто цю інформацію банк обробляє на підставі договору.

Нагадаємо, що персональні дані мають бути точними, достовірними та оновлюватися за потреби, визначеної метою їх обробки (ст. 6 Закону № 2297 [137]). Тому якщо банк отримав у договорі право на обробку певних даних, він

повинен підтримувати їх в актуальному стані – якщо це відповідає меті договору. А тому тільки з цією метою банк може звертатися до роботодавця, щоб актуалізувати інформацію – тільки в строки та з метою виконання договору. Саме тому, якщо працівник підтвердив, що згоден на передання такої інформації, то роботодавець може задовольнити такий запит банку.

Актуальним нині є питання проведення аудиторських перевірок. Відтак, часто виникає запитання – а чи надавати особові картки та особові справи аудиторській компанії, що проводить аудит підприємства? У таких випадках роботодавець може надавати документи з персональними даними лише за згоди працівника. Якщо такої згоди роботодавець не отримав, то слід надавати аудиторам довідки зі знеособленою інформацією. Адже особові картки та особові справи містять персональні дані працівників.

Суб'єкти господарювання проходять аудит, наприклад, перед поданням консолідованої фінансової звітності на договірних засадах. До так званої «Великої четвірки» аудиторських компаній належать KPMG, Ernst&Young, Delloit, PwC.

Ані Закон № 2297 [137], ані будь-який інший законодавчий акт не дозволяє надавати персональні дані працівників без їх згоди на запит аудиторських компаній. До того ж роботодавці не можуть надавати персональні дані працівників навіть на запит Держаудитслужби, оскільки працівники не є предметом аудиту. Відтак, вимоги аудиторів: надати оригінали чи копії особових справ працівників та особових карток П-2 – неправомірні. Таким чином, роботодавець може надати аудитору документи з персональними даними, якщо отримає попередню згоду працівників на передавання їх персональних даних. Якщо роботодавець не отримав згоди, то доцільно підготувати довідку про освіту, підвищення кваліфікації та досвід роботи працівників зі знеособленою інформацією.

Наведемо приклад ситуації. У роботодавця під час аудиторської перевірки зі стандартів IFS і BRC вимагали надати особові картки та особові справи працівників. Відтак, виникло справедливе запитання – чи виконувати таку вимогу?

Аудиторські перевірки зі стандартів IFS (*International Food Standard*) і BRC (*British Retail Consortium*) підприємств харчової промисловості проводять з метою контролю дотримання їх вимог:

– відповідальності топ-менеджерів з якості та безпечності харчових продуктів;

– системи HACCP (*Hazard Analysis and Critical Control Point*);

– гігієни персоналу, кваліфікації та навчання працівників;

– гігієни виробничих операцій та інфраструктури;

– контролю якості та безпеки виробів.

Ані Закон № 2297 [137], ані будь-який інший законодавчий акт не дозволяє підприємству харчової промисловості надавати персональні дані працівників без їх згоди для перевірки зі стандартів IFS і BRC. А особові картки та особові справи містять персональні дані працівників. Тому роботодавець може надати аудитору документи з персональними даними, якщо отримає попередню згоду працівників на передавання їх персональних даних. Якщо роботодавець не отримав згоди, то варто підготувати довідку про освіту, підвищення кваліфікації та досвід роботи працівників зі знеособленою інформацією [183].

Останніми роками водночас актуальними та складними залишаються питання військового обліку. Відтак, виникає безліч запитань щодо передання даних про працівників. Зокрема, одним із таких питань є надання на вимогу територіальних центрів комплектування та соціальної підтримки (далі – ТЦК та СП) відомостей про працівників, які працюють на транспортних засобах підприємства. Дійсно, ТЦК та СП має право отримати від роботодавця цю інформацію.

Отже, щоб визначити, чи правомірно передати такі відомості про фізичну особу, маємо з’ясувати:

1) чи передбачено можливість або необхідність передання відомостей певним законом;

2) чи є інтереси національної безпеки, економічного добробуту та прав людини.

У наведеній ситуації маємо таке:

1.Чи передбачено можливість або необхідність передання відомостей певним законом?

Запитуючи інформацію про транспортні засоби, ТЦК та СП діє відповідно до Закону України № 3543 [141]). Так, ст. 6 зазначеного Закону передбачає військово-транспортний обов'язок підприємств, установ та організацій усіх форм власності. Мета військово-транспортного обов'язку – задоволення потреб ЗСУ, інших військових формувань на особливий період транспортними засобами і технікою. Обов'язок поширюється:

– на центральні та місцеві органи виконавчої влади, інші державні органи, органи місцевого самоврядування, підприємства, зокрема на залізниці, порти, пристані, аеропорти, нафтобази, автозаправні станції дорожнього господарства та інші підприємства, які забезпечують експлуатацію транспортних засобів;

– на громадян – власників транспортних засобів.

Керівники підприємств подають ТЦК та СП щороку до 20 червня та 20 грудня інформацію про наявність транспортних засобів і техніки, їх технічний стан, а також про громадян, які працюють на підприємствах на таких транспортних засобах і техніці (п. 15 Положення про військово-транспортний обов'язок (далі – Положення № 1921 [132]). Форма звіту затверджена додатком 1 до Положення № 1921.

У звіті зазначають інформацію про директора, заступника директора (головного інженера), начальника (працівника) кадрової служби, їх номери телефонів, місце проживання, список транспортних засобів і техніки, закріплених за ними громадян тощо.

Отже, Положення № 1921 [132], розроблене на виконання Закону України № 3543-XII [141], та передбачає необхідність подавати до ТЦК та СП відомості не тільки про транспортні засоби, але й про громадян, які працюють на цих засобах.

2. Чи є інтереси національної безпеки, економічного добробуту та прав людини?

Передання таких відомостей до ТЦК та СП обумовлено інтересами національної безпеки. Адже підготовка й утримання в належному стані техніки та об'єктів, призначених для передачі в разі мобілізації ЗСУ, іншим військовим формуванням є одним зі складників мобілізаційної підготовки (ч. 3 ст. 3 Закону України № 3543-XII [141]), а мобілізаційна підготовка є складником комплексу заходів для оборони держави (ч. 1 ст. 3 Закону України № 3543-XII [141]).

Наведемо ще одну практичну ситуацію. Роботодавець вчасно подав повідомлення про зміну облікових даних, тож виникло питання – чи надавати ТЦК та СП копію наказу про звільнення працівника? У цьому випадку роботодавець не зобов'язаний надавати витяг із наказу про звільнення працівника, оскільки роботодавець вже виконав обов'язок і подав повідомлення про зміну облікових даних.

Роботодавець у 5-денний строк надсилає до ТЦК та СП повідомлення про зміну облікових даних призовників і військовозобов'язаних (далі – Повідомлення), звільнених з роботи (п. 34 Порядку № 1487 [134]). У такому випадку роботодавець зазначає назву, номер та дату видання документа, який став підставою для зміни облікових даних. Копію чи витяг із наказу роботодавець не зобов'язаний надсилати ТЦК та СП, як і повідомляти причину звільнення. Окремо прописаний обов'язок роботодавця повідомляти про призначення, переміщення і звільнення керівного складу та осіб, відповідальних за ведення військового обліку (п. 13 Порядку № 1487 [134]). Однак, подавати копії документів чи витяги з них не передбачено.

Законодавство дає змогу представникам ТЦК та СП ознайомитися з наказами під час перевірки (Додаток 31 до Порядку № 1487 [134]), але також не передбачає їх копіювання.

Таким чином, так як законодавство у сфері військового обліку не містить ані обов'язку роботодавця надавати копію наказу про звільнення працівника, ані права ТЦК та СП вимагати його, то роботодавець має право відмовити ТЦК та СП.

Наведемо ще одну спірну ситуацію. ТЦК та СП вимагало від роботодавця копію трудової книжки, характеристику й автобіографію працівника. Виникло запитання – чи надавати ці документи? Вважаємо, що якщо працівник не просив роботодавця надати документи до ТЦК та СП, то роботодавець не має права цього робити. Адже запит ТЦК та СП з вимогою надати копію трудової книжки, характеристику чи автобіографію є, по суті, вимогою про первинні документи кандидата на військову службу за контрактом. Зазвичай, працівники самі надають до ТЦК та СП всі необхідні документи, але часто працівники вчиняють до досить прозоро щодо роботодавця. Тож працівники часто говорять ТЦК та СП запитати ці документи у роботодавця. Наміри працівника: (1) заздалегідь не виправдовуватись перед роботодавцем, адже не факт, що з ним укладуть контракт; (2) не втратити робоче місце до укладання контракту.

Законодавство у сфері військового обліку не містить обов'язку роботодавця надавати жоден із документів, як і права ТЦК та СП вимагати їх. Тому роботодавцю у такій ситуації доцільно зазначити, що повідомив працівника про запит та запропонував за його вимогою виготовити копію трудової книжки й підготувати характеристику. Автобіографію працівник складає власноруч у довільній формі, або за зразком, наданим у ТЦК та СП.

Цікавими на практиці є ситуації щодо надання персональних даних працівників на запити поліції. У роботодавців завжди виникає дилема – що робити у таких випадках, чи надавати такі відомості?

Зауважимо, що Нацполіція може надіслати запит щодо інформації або копій документів, що містять персональні дані працівників, за однією з підстав:

– оперативно-розшукова діяльність;

– кримінальне провадження (ст. 23 Закону України № 580 [142]).

1.Запити у зв'язку з проведенням оперативно-розшукової діяльності.

У запиті Нацполіції про надання інформації або копій документів, що містять персональні дані, має бути номер оперативно-розшукової справи та

правові підстави для такого запиту, визначені ч. 1 ст. 6 Закону України № 2135 [143]).

Оперативно-розшукову діяльність мають право здійснювати підрозділи кримінальної та спеціальної Нацполіції (абз. 2 ч. 1 ст. 5 Закону України № 2135 [143]). Якщо є підстави для оперативно-розшукової діяльності, Нацполіція заводить оперативно-розшукову справу (ч. 1 ст. 9 Закону України № 2135 [143]).

Підстави для оперативно-розшукової діяльності встановлені ч. 1 ст. 6 Закону України № 2135 [143]:

1) наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів, про:

– злочини, що готуються;

– осіб, які готують вчинення злочину;

– осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання;

– осіб безвісно відсутніх;

– розвідувально-підривну діяльність спецслужб іноземних держав, організацій та окремих осіб проти України;

– реальну загрозу життю, здоров'ю, житлу, майну працівників суду і правоохоронних органів у зв'язку з їх службовою діяльністю, а також осіб, які беруть участь у кримінальному судочинстві, членів їх сімей та близьких родичів, з метою створення необхідних умов для належного відправлення правосуддя; співробітників розвідувальних органів України у зв'язку із службовою діяльністю цих осіб, їх близьких родичів, а також осіб, які конфіденційно співробітничають або співробітничали з розвідувальними органами України, та членів їх сімей з метою належного здійснення розвідувальної діяльності;

2) запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках;

3) потреба в отриманні розвідувальної інформації в інтересах безпеки суспільства і держави;

4) наявність узагальнених матеріалів центрального органу виконавчої влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму, отриманих в установленому законом порядку.

2. Запити у зв'язку з кримінальним провадженням.

Нацполіція уповноважена проводити досудове розслідування кримінальних правопорушень у межах визначеної підслідності (п. 6 ч. 1 ст. 23 Закону України № 580 [142]).

Якщо щодо працівника порушено кримінальне провадження, Нацполіція отримує доступ до документів чи їх копій, що містять персональні дані працівника, у порядку, визначеному главою 15 Кримінального процесуального кодексу України (далі – КПК України [102]). Тимчасовий доступ до речей і документів надається на підставі ухвали слідчого судді, суду (ч. 2 ст. 159 КПК України [102]).

У випадку подання клопотання про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю, сторони кримінального провадження зобов'язані довести можливість використання як доказів відомостей, що містяться в речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів (п. 6 ч. 2 ст. 160 КПК України, ч. 6 ст. 163 КПК України [102]).

Персональні дані особи, що знаходяться в її особистому володінні або в базі персональних даних володільця персональних даних, віднесено до охоронюваної законом таємниці (п. 8 ч. 1 ст. 162 КПК України [102]). Тож в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів має бути зазначено:

– прізвище, ім'я та по батькові особи, якій надається право тимчасового доступу до речей і документів;

– дата постановлення ухвали;

– положення закону, на підставі якого постановлено ухвалу;

– прізвище, ім’я та по батькові фізичної особи або найменування юридичної особи, які мають надати тимчасовий доступ до речей і документів;

– назва, опис, інші відомості, які дають можливість визначити речі й документи, до яких повинен бути наданий тимчасовий доступ;

– розпорядження надати (забезпечити) тимчасовий доступ до речей і документів зазначеній в ухвалі особі, а також надати їй можливість вилучити зазначені речі й документи, якщо відповідне рішення було прийнято слідчим суддею, судом;

– строк дії ухвали, який не може перевищувати одного місяця з дня постановлення ухвали;

– положення закону, які передбачають наслідки невиконання ухвали слідчого судді, суду (підстава – ст.164 КПК України [102]).

Особа, яка зазначена в ухвалі як володілець речей або документів, зобов’язана надати тимчасовий доступ до зазначених в ухвалі речей і документів особі-запитувачу, вказаній в ухвалі (ч. 1 ст. 165 КПК України [102]).

Відтак, якщо надання персональних даних працівників на запити поліції здійснюються з вищенаведеними цілями та у названих випадках, то надання роботодавцем цих відомостей буде правомірним та не порушуватиме чинне законодавство про захист персональних даних працівників.

Схожої думки ми дотримуємося і випадку надання персональних даних працівників на письмовий запит прокуратури. За загальним правилом, роботодавець може надавати такі відомості за згодою працівника. Якщо згоди немає, то надавати можна якщо в письмовому запиті прокуратури обґрунтовані його мета та (або) правові підстави.

Зауважимо, що при здійсненні прокурорського нагляду за додержанням і застосуванням законів прокурор має право, зокрема: мати доступ до документів і матеріалів; письмово вимагати подання в прокуратуру документів та матеріалів, видачі необхідних довідок тощо (ст. 23 Закону України № 1697 [149]).

Отже, володілець персональних даних може не надати інформацію на запит прокуратури, якщо:

1) у запиті немає посилання на відповідні статті, що обґрунтовують обов'язковість надання такої інформації;

2) не додано копії документів із підставами, що свідчать про можливі порушення законності;

3) не має обґрунтування необхідності вчинення відповідних дій.

Володілець персональних даних може надавати органам прокуратури інформацію щодо займаної посади працівників та з якого часу працівники на ній перебувають, оскільки така інформація не є конфіденційною, однак тільки якщо запит оформлений згідно з вимогами ч. 4 ст. 16 Закону № 2297 [137]. Адже законні вимоги прокурора є обов'язковими для всіх органів, підприємств, установ, організацій, посадових осіб та громадян і виконуються невідкладно або у передбачені законом чи визначені прокурором строки. Ухилення від виконання законних вимог прокурора тягне за собою відповідальність, передбачену законом.

Наразі актуальним є передання відомостей до органів Пенсійного фонду України. Наведемо ситуацію. Так, ПФУ надіслав запит роботодавцю щодо надання документів, що підтверджують достовірність довідок про зарплату колишнім працівникам. Вважаємо, що роботодавець може надати такі документи, якщо в запиті вказана мета – інвентаризація пенсійних справ.

Нагадаємо, що з 2018 року ПФУ проводить інвентаризацію пенсійних справ, метою якої є перевірка правильності призначення та виплати пенсій, розвиток електронних пенсійних справ на базі централізованих інформаційних технологій правління ПФУ. Пенсійні справи інвентаризують за порядком, затвердженим постановою Правління ПФУ від 03.09.2018 р. № 19-1 (далі – Порядок № 19-1 [148]). Керівник органу ПФУ створює інвентаризаційну комісію (п. 4 розд. І Порядку № 19-1 [148]), яка перевіряє і підтверджує документально:

– фактичну наявність пенсійних справ одержувачів пенсій (щомісячного довічного грошового утримання), їх відповідність базі даних і даним контрольно-інвентаризаційної відомості;

– наявність необхідних документів у пенсійній справі;

– правильність обчислення розміру пенсійних виплат, зокрема з урахуванням відомостей бази даних;

– відповідність відомостей пенсійної справи інформації, що обробляється в базі даних (прізвище, ім'я, по батькові, дата народження, група, підгрупа, причина та строк, на який встановлено інвалідність одержувача пенсії (щомісячного довічного грошового утримання), непрацездатних членів його сім'ї, померлих годувальників, місце проживання (перебування), реєстраційний номер облікової картки платника податків (РНОКПП) або серія та номер паспорта чи іншого документа, що посвідчує особу (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку в паспорті), тощо);

– дотримання порядку відшкодування надміру виплачених сум пенсій, що підлягають поверненню;

– наявність виконавчих документів, на підставі яких відраховують із пенсії;

– правильність визначення дати, до якої слід провести відрахування;

– відповідність виплачених сум розмірам призначеної (перерахованої) пенсії (щомісячного довічного грошового утримання) та здійснених з неї утримань, відрахувань (п. 2 розділу ІІ Порядку № 19-1 [148]).

Відповідно чи правильно обчислено розмір пенсійних виплат, перевіряють після того, як з'ясують повноту і достовірність наявних у пенсійній справі документів (п. 3 розд. ІІ Порядку № 19-1 [148]). Так, якщо при обчисленні пенсії враховано зарплату за періоди до 01.07.2000 за сумісництвом, інвентаризаційна комісія перевіряє, чи є документи, що підтверджують роботу за сумісництвом (абз. 1 п. 6 розд. ІІ Порядку № 19-1

[148]). А ось за довідками, виданими з 01.01.1992, за якими в помісячному розрахунку розмір зарплати або сума доходу перевищує 5,6 розміра середньої зарплати в Україні на день отримання зазначених сум, перевіряють обґрунтованість їх видання та відповідність зазначених у них сум зарплат (доходу) первинним документам. А умовою надання таких відомостей стане відсутність в пенсійній справі матеріалів перевірки (абз. 2 п. 6 розд. II Порядку № 19-1 [148]).

Наразі часто при передачі документів до ПФУ, вимагають ще й копії паспорта працівника. Відтак, роботодавці вагаються чи не стане це порушенням законодавства про захист персональних даних працівників. На нашу думку, ПФУ немає правових підстав для запиту копії паспорта працівника, а у відповідь ПФУ роботодавець може вказати, що відмова не є перешкоджанням державному органу здійснювати свої повноваження, а — лише дотримання норми ч. 1 ст. 24 Закону № 2297 [137]. А саме, дотримання обов'язку володільця, розпорядника персональних даних щодо забезпечення захисту цих даних від випадкових втрати або знищення, від незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних. Також роботодавцю доречно зазначити, що він повідомив працівника про запит та рекомендував найближчим часом звернутись до ПФУ з оригіналом паспорта та його копією.

А ось отримувати згоду працівників на обробку персональних даних для передавання сканів трудових до ПФУ не потрібно. ПФУ вимагав згоду на обробку персональних даних відповідно до Закону № 2297 [137] та Постанови КМУ від 27.11.2019 р. № 1084 [127], допоки не набрав чинності Закон України «Про внесення змін до деяких законодавчих актів України щодо обліку трудової діяльності працівника в електронній формі» від 05.02.2021 № 1217-IX (далі – Закон № 1217 [123]). Відтак, Закон № 1217 [123] зобов'язав ПФУ переводити відомості про трудову діяльність в електронний формат, чим надав дозвіл на обробку персональних даних. Тож окрема згода працівника для цього не потрібна.

Важливим та не менш дискусійним залишається запитання – чи надавати персональні дані працівника на запит адвоката? Адвокати найчастіше звертаються до відділу кадрів із вимогою надати відомості про працівника, який фігурує у справі про призначення аліментів.

Адвокати мають право звертатися з адвокатськими запитами, зокрема щодо отримання копій документів, до органів державної влади, ОМС, їх посадових і службових осіб, підприємств, установ, організацій, громадських об'єднань, а також до фізичних осіб (за згодою таких фізичних осіб). Для адвокатських запитів передбачено вимоги щодо їх оформлення і порядок їх подання (ст. 20 та 24 Закону України № 5076 [119]).

Відмова у доступі до персональних даних можлива, якщо доступ до них заборонено згідно із законом (ч. 3 ст. 24 Закону № 5076 [119]). Орган державної влади, ОМС, їх посадові та службові особи, керівники підприємств, установ, організацій, громадських об'єднань зобов'язані не пізніше п'яти робочих днів із дня отримання адвокатського запиту надати адвокату відповідну інформацію, копії документів. Винятком є інформація з обмеженим доступом і копії документів, в яких міститься інформація з обмеженим доступом (ст. 24 Закону № 5076) [119].

Отже, відмова надати інформацію на адвокатський запит, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, тягнуть за собою відповідальність, встановлену законом, крім випадків відмови в наданні інформації з обмеженим доступом.

Наведемо ситуацію. Чи можна передати персональні дані колишнього працівника юридичної фірмі, що представляє роботодавця у трудовому спорі. Вважаємо, що можна, але слід дотриматися вимог у сфері захисту персональних даних. У зазначеній ситуації отримувати окрему згоду від колишнього працівника на обробку його персональних даних юридичною фірмою, яка представлятиме інтереси підприємства в суді, не потрібно, але слід повідомити особу про те, що роботодавець передає її персональні дані юридичній фірмі.

Вимоги, яких має дотриматися роботодавець:

1. Визначити статус юридичної фірми в контексті Закону № 2297 [137] — розпорядник персональних даних чи третя особа. Доречно визначити юридичну компанію як розпорядника. Володілець персональних даних може доручити обробку персональних даних розпоряднику відповідно до договору, укладеного в письмовій формі. Розпорядник персональних даних може обробляти їх лише з метою і в обсязі, визначеними в договорі (ст. 4 Закону № 2297 [137]). І саме у договорі з юридичною фірмою – розпорядником персональних даних, доречно врегулювати всі питання обробки персональних даних.

2. Повідомити письмово особу про передання її персональних даних юридичній фірмі. Так роботодавець дотримається вимог статей 8 та 12 Закону № 2297 [137]. Хоча ст. 12 Закону № 2297 [137] не вимагає повідомляти письмово, але, ми переконані, що це підтвердить, що роботодавець дотримався закону.

Нині актуальними є питання відновлення втрачених документів. Саме тому наразі часто до роботодавців звертається ДМС із запитом про надання персональних даних працівника, який втратив паспорт.

Працівник або колишній працівник – суб’єкт персональних даних може:

– надати згоду (доручення) на передачу своїх персональних даних ДМС для оформлення паспорта замість втраченого. Якщо є заява, роботодавець може надати ДМС копії (витяги) документів;

– звернутися до роботодавця з заявою надати йому особисто копії документів, що містяться в особовій справі. Роботодавець надсилає на адресу ДМС лист-відмову, а необхідні документи надає працівнику.

Суб’єкт персональних даних має право отримати відповідь про те, чи обробляються його персональні дані, а також зміст таких персональних даних. Строк надання відповіді — не пізніш як за 30 календарних днів з дня надходження запиту, крім випадків, передбачених законом (ч. 2 ст. 8 Закону України № 2297 [137]).

Якщо запит оформлено як належить, роботодавець зобов'язаний вивчити його для задоволення. Строк для вивчення – 10 робочих днів із дня надходження запиту (ч. 5 ст. 16 Закону № 2297 [137]).

Після прийняття до розгляду заяви-анкети про оформлення паспорта замість втраченого (викраденого) та доданих до неї документів працівник територіального органу чи територіального підрозділу ДМС вживає заходів з ідентифікації особи, на ім'я якої оформляється паспорт (п. 49 Порядку від 25.03.2015 № 302; далі – Порядок № 302 [129]).

ДМС має право отримувати інформацію про особу з наявних державних та єдиних реєстрів, інших інформаційних баз, що перебувають у власності держави або підприємств в обсязі, необхідному для ідентифікації особи у зв'язку з оформленням (зокрема, замість втраченого або викраденого), обміном паспорта (п. 16 Порядку № 302 [129]).

ДМС проводить процедуру встановлення особи, якщо картотеки заяв про видачу паспорта територіального підрозділу ДМС не збереглися, відсутня будь-яка інформація в даних обліку територіального органу ДМС (п. 62 Порядку № 302 [129]).

ДМС надсилає запити щодо перевірки документів та інформації, зазначеної заявником у письмовому зверненні, зокрема до МВС, Національної поліції, Мін'юсту, органів ДФС, навчальних закладів, військових частин, військових комісаріатів, установ виконання покарань, щоб отримати інформацію з наявних державних та єдиних реєстрів, інших інформаційних баз, що перебувають у власності держави або підприємств, зокрема фотокартки особи, яка дасть змогу ідентифікувати особу. Під час перевірки ДМС бере до уваги всю інформацію, яку повідомив заявник (п. 43 Порядку № 302 [129]).

Якщо ДМС у запиті посилається на пункти 43 та 62 Порядку № 302 [129], то роботодавець може надати запитувану інформацію. Однак, попередньо варто погодити це з працівником. Якщо роботодавець не має згоди працівника на передання персональних даних, то слід написати листа-відповідь ДМС із відмовою. У листі-відповіді варто зауважити, що відмова не є

перешкоджанням державним органам у здійсненні своїх повноважень, а лише дотриманням норми ч. 1 ст. 24 Закону № 2297 [137], зокрема обов'язку володільця, розпорядника персональних даних захищати їх від випадкових втрати або знищення, від незаконного оброблення, зокрема незаконного знищення чи доступу до них.

А ось щодо прохання працівника передати ДМС наказ про прийняття вайбером, зазначимо наступне. Працівник сам може надати наказ ДМС, а роботодавець може зробити це тільки за письмовою заявою працівника.

Зауважимо, що якщо ДМС не надсилала роботодавцю запиту надати копію наказу про прийняття працівника, то у цій ситуації працівник – суб'єкт персональних даних може:

– надати згоду (доручення) на передавання своїх персональних даних ДМС. Якщо є заява, роботодавець може надіслати ДМС листом завірену копію наказу;

– звернутися до роботодавця з заявою надати йому особисто копію наказу. Роботодавець надає працівникові завірену копію наказу про прийняття.

Вважаємо, що роботодавцю у такій ситуації не варто надавати персональні дані на усне прохання працівника, а тим більше передавати його фотокопію Вайбером за номером телефону, який він надав. Якщо з часом працівник поскаржиться, що роботодавець безпідставно передав його персональні дані іншій особі, працівник кадрової служби не матиме документального підтвердження, що він це зробив на його прохання.

Складним на практиці є вирішення питання надання/не надання ідентифікаційних номерів працівників на запит Антимонопольного комітету України. На нашу думку, роботодавцеві можна надати їх, якщо Антимонопольний комітет України (АМКУ) вказав у запиті, які саме дані про працівників його цікавлять і правову підставу для запиту.

Попри те, що такі відомості про індивідуальні ідентифікаційні номери працівників є інформацією з обмеженим доступом, роботодавець повинен їх повідомити, навіть без згоди суб'єкта персональних даних. Адже АМКУ має

повноваження при розгляді заяв і справ про порушення законодавства про захист економічної конкуренції, при перевірці вимагати від суб'єктів господарювання, їх посадових осіб і працівників інформацію, зокрема з обмеженим доступом (п. 5 ч. 1 ст. 7 Закону України «Про Антимонопольний комітет» від 26.11.1993 р. № 3659-XII [120]).

З метою дотримання мінімальних стандартів у сфері оплати праці часто робоча група з легалізації зарплати та детінізації зайнятості надсилає роботодавцям запит про надання інформації про зарплату менше мінімальної, яка виплачується працівникам. На наше переконання, роботодавець має підготувати такі документи для надання. Якщо в запиті згадали конкретних працівників, то слід переконатися, що запит відповідає вимогам із захисту персональних даних.

Ще у 2010 р. було затверджено План заходів щодо детінізації доходів та відносин у сфері зайнятості населення [131], яким утворено регіональні, районні та міські робочі групи з питань легалізації виплати заробітної плати та зайнятості населення, зокрема ці групи утворили при районних державних адміністраціях (далі – РДА). Повноваження РДА в галузі зайнятості населення, праці та зарплати визначає ст. 24 Закону України «Про місцеві державні адміністрації» (далі – Закон № 586 [140]).

Місцева державна адміністрація (далі – МДА), зокрема:

– забезпечує реалізацію державних гарантій у сфері праці, зокрема й на право своєчасного одержання винагороди за працю;

– розробляє та здійснює заходи щодо реалізації державної політики зі сприяння зайнятості населення на рівні регіону;

– забезпечує реалізацію державних гарантій у сфері праці (ст. 24 Закону № 586 [140]).

Для реалізації повноважень МДА мають право:

– проводити перевірки, чи додержують Конституції та законів, інших актів законодавства ОМС та їх посадові особи, керівники підприємств, установ, організацій, їх філіалів та відділень незалежно від форм власності й підпорядкування за напрямами, визначеними ст. 16 Закону № 586 [140];

– одержувати відповідну статистичну інформацію та інші дані від підприємств, установ та організацій, їх філіалів і відділень незалежно від форм власності (ст. 28 Закону № 586 [140]).

МДА в межах, визначених Конституцією і законами України, здійснюють на відповідних територіях державний контроль, зокрема, за охороною праці та своєчасною, і не нижче визначеного державою, мінімального розміру оплатою праці (п. 10 ч. 1 ст. 16 Закону № 586 [140]).

Голова МДА:

– утворює консультативні, дорадчі та інші допоміжні органи (ради, колегії, робочі групи тощо), служби й комісії;

– визначає завдання, функції та персональний склад таких органів (п. 9 ч. 1 ст. 39 Закону № 586 [140]; п. 43 Типового регламенту місцевої державної адміністрації [135].

Отже, керівник управління соціального захисту населення (далі — УСЗН), як член районної робочої групи з питань легалізації виплати зарплати та зайнятості населення може запитувати у роботодавців інформацію про зарплату, якщо є факти виплати працівникам зарплати, нижче мінімальної.

Якщо запитувана інформація окрім знеособлених статистичних даних містить інформацію про персональні дані працівників, то варто готувати відповідь на запит з огляду на Закон України № 2297 [137].

Якщо УСЗН указав усю необхідну інформацію, зокрема, є посилання на норми Закону № 586 [140], то роботодавець має підготувати запитувану інформацію [183].

Залишаються проблемними питання щодо використання відеоконтролю за працівниками. Правила обробки персональних даних у сфері працевлаштування повинні містити чіткі заходи щодо захисту людської гідності, законних інтересів та основоположних прав працівників [52, с. 9]. Водночас особливе значення надається прозорості та чіткості процедур моніторингу на робочому місці, адже сьогодні поширеною проблемою є законний ступінь контролю за електронною комунікацією працівника. Абсолютна заборона на використання засобів зв’язку на роботі із приватною

метою є нереальним та непропорційним кроком. Зважаючи на це роботодавці повинні дотримуватись спеціальних правил обробки персональних даних, які отримані ними під час виконання працівниками трудових обов'язків. Зокрема, встановлення кожної камери спостереження за працівниками вимагає обґрунтування законного інтересу роботодавця для таких дій. Якщо цей інтерес зумовлюється потребою захистити право власності роботодавця, то вважатиметься правомірним і, таким чином, матиме перевагу над інтересом працівника щодо захисту його приватності. Однак треба завжди враховувати те, чи можна досягнути цієї ж мети з меншим утручанням у приватне життя працівника. Наприклад, скерувати камери на вхідні двері до приміщення, а не на робочі місця. Адже право на захист персональних даних не є абсолютним правом, воно повинно розглядатись у зв'язку з його функцією в суспільстві та бути збалансованим з іншими фундаментальними правами відповідно до принципу пропорційності [181, с. 237].

У цьому контексті на рівні ЄС поки без вирішення залишається питання моніторингу дистанційних працівників. Контроль їхнього робочого часу за допомогою засобів роботодавця, які записують натискання клавіш чи рух комп'ютерної миші, ідентифікують активність екрану, активують процес запису веб-камер чи мікрофона навряд чи вважатиметься допустимим та пропорційним меті збору інформації. Якщо ж відповідне обладнання належить працівнику, то розміщення на них будь-яких засобів моніторингу потенційно можуть бути кваліфіковані як злочин [52, с. 16].

Чи не найбільш проблемним є автоматизований моніторинг. Розпізнавання рис та міміки обличчя працівників, як правило, вважається незаконним. Дискусійним є використання біометричних даних особи для доступу до робочого місця. Оскільки на комунітарному рівні чітких інструкцій з цього питання немає, то держави-члени можуть створювати власні правила в контексті обробки біометричних даних працівників.

Регламент (ЄС) 2016/679 зобов'язує роботодавця повідомляти працівників про те, яку інформацію про них він може обробляти, як буде здійснюватись ця обробка та якими правами працівники володіють щодо

захисту власної приватності. Зробити це можна за допомогою локальної заяви про конфіденційність чи локальних умов політики приватності. Останні повинні безумовно визначати підстави застосування моніторингу на робочому місці, мету обробки даних, указувати на засоби моніторингу та місця їхнього розташування, давати вказівку на тривалість зберігання даних, з огляду на їхній вид, перелік суб'єктів із доступом до даних та підстави доступу, правила захисту даних, права працівників. Ці умови повинні бути легкодоступними для всіх працівників. Їх також повідомляють кожному новому працівнику або ж надають доступ до електронних ресурсів, де б можна було із цими правилами ознайомитись.

Законною та виправданою перевіркою персональних даних можна вважати моніторинг роботодавцем профілів його колишніх працівників у LinkedIn, щодо яких діють обмеження конкуренції після припинення трудових відносин. Адже метою відповідної обробки персональних даних є контроль за дотриманням відповідних конкурентних обмежень та здійснюється він лише щодо колишніх працівників. Належним чином засвідчена поінформованість працівника про регулярність вивчення роботодавцем його публічних дописів є ще однією умовою законності здійснення відповідного моніторингу [52, с. 12].

Взявши до уваги те, що перевірка даних про працівника може здійснюватись роботодавцем майже постійно, адже новітні технології забезпечують перманентний доступ до профілів працівників у соціальних мережах, запроваджено правило, за яким перевірка персональних даних працівників не може вважатись виправданою, якщо здійснюється на узагальнених підставах [50, с. 14].

Важливо наголосити на тому, що інформація, отримана роботодавцем про особу, котра шукає роботу, повинна бути знищена, як тільки стане зрозуміло, що особі не буде зроблено пропозицію обійняти вакантну посаду або ж особа відмовляється від запропонованої посади [152, с. 223-224].

На практиці роботодавці дуже часто звертаються до медичних закладів щодо надання останніми інформації про перебування на лікуванні певного

працівника, підтвердження або спростування інформації про стан тимчасової непрацездатності працівника. Та чи можуть роботодавці звертатися про витребування такої інформації? І чи мають право медичні установи надавати таку інформацію?

Для пошуку відповідей на ці питання та наукового обґрунтування, звернемося до судової практики. Так, позивач перебував у трудових відносинах з ПАТ «Полтаваобленерго», займав посаду директора з правової роботи та надавав згоду на обробку його персональних даних при прийнятті на роботу.

ПАТ «Полтаваобленерго» запитувало в медичних закладах інформацію щодо наданих позивачем (їх працівником) листків непрацездатності, у яких були зазначені назви установ, що їх видавали, періоди проходження лікування.

Відповідні запити до медичних установ ПАТ «Полтаваобленерго», здійснювало з метою підтвердити чи спростувати інформацію, подану самим позивачем до Ленінського районного суду м. Полтави в рамках іншої цивільної справи, відкритої за його позовною заявою, в якій він зазначав, що в період червня–жовтня 2015 року він постійно звертався до медичних закладів з метою отримання лікування.

Також відповідно до табелю обліку робочого часу за вересень 2018 року, працівник (позивач), на момент подання відповідних запитів був тривалий час відсутній на роботі, у зв`язку з чим роботодавець звернувся до відповідних медичних установ з запитами про надання інформації.

При цьому відповідач – ПАТ «Полтаваобленерго» стверджував у суді, що не зверталося до медичних закладів з питань надання інформації щодо стану здоров`я, характеру захворювання та лікування. Запити, які направляло товариство, містили інформацію про особу, яка вже була ідентифікована, зокрема прізвище, ім`я, по батькові, дату народження, місце реєстрації, а також період, в який ця особа могла звертатися до медичних установ.

У свою чергу позивач в обґрунтування позовних вимог вказував, що з урахуванням змісту кожного запиту ПАТ «Полтаваобленерго» та відповіді

медичних установ на запит, було порушено його право на захист персональних медичних даних, тобто було здійснено обробку таких даних без його згоди.

Відмовляючи у задоволенні позовних вимог позивача до ПАТ «Полтаваобленерго», суд першої інстанції виходив з того, що здійснені вказаним товариством, як роботодавцем, запити відносно працівника із зазначенням його персональних даних, як суб`єкта персональних даних, який не обмежував роботодавця у використанні власних персональних даних, і які не виходять за межі встановленої законом заборони, – не суперечать вимогам Закону України «Про захист персональних даних» та не порушили права позивача на захист персональних даних, також права на таємницю про стан здоров`я.

Судом першої інстанції визначено, що позивач – працівник є суб`єктом персональних даних. ПАТ «Полтаваобленерго» вважається володільцем персональних даних працівника – позивача, з огляду на укладений з останнім трудовий договір і перебування сторін у трудових правовідносинах.

Виходячи із приписів Закону України «Про захист персональних даних», суд зробив висновок, що роботодавець, як володілець персональних даних працівника, з яким укладено трудовий договір, має право на обробку персональних даних такого працівника, в частині, що не заборонена законом, і згода суб`єкта персональних даних на обробку його персональних даних, у розумінні абзацу 4 ст. 2 Закону «Про захист персональних даних», – не вимагається.

Обов`язковою вимогою у процедурі обмеження суб`єктом персональних даних доступу до його персональних даних володільцю, за змістом ст. 8 Закону України «Про захист персональних даних», є письмова заява такого суб`єкта надана володільцю бази даних, її розгляд адміністрацією володільця та прийняття рішення щодо такої заяви.

Медичні заклади, визначені у справі відповідачами, до яких позивач звертався як пацієнт за медичною допомогою і яким у зв`язку із цим надавав свої персональні дані, у розумінні Закону України «Про захист персональних даних» також вважаються володільцями персональних даних останнього,

однак, підстави їх обробки будуть іншими, ніж у володільця, з яким суб`єкт персональних даних перебуває у трудових правовідносинах.

У даному випадку, відповідно до вимог п. 1 ч. 1 ст. 11 Закону України «Про захист персональних даних», необхідне отримання згоди суб`єкта персональних даних на обробку його персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.

При цьому медичні заклади у зв`язку зі зверненням фізичних осіб за медичною допомогою, лікуванням, є володільцями конфіденційної інформації про фізичну особу (стан здоров`я, діагноз, методи лікування, медичне обстеження, огляд та їх результати, інтимна і сімейна сторони життя громадянина), віднесеної Законом України «Основи законодавства України про охорону здоров`я» до лікарської таємниці.

Із досліджених судом першої інстанції запитів ПАТ «Полтаваобленерго» щодо позивача та наданих на них відповідей медичних установ м. Полтави (відповідачів у справі), встановлено, зокрема, що згідно із запитом ПАТ «Полтаваобленерго», адресованого головному лікарю Другої міської клінічної лікарні, роботодавцем запитувалась інформація щодо працівника (позивача) з приводу листка непрацездатності, який був наданий останнім роботодавцю; у зв`язку із тим, що в листку непрацездатності не зазначена дата, з якої працівнику необхідно приступити до роботи, – запитувалась інформація про знаходження працівника на лікуванні у медичному закладі. Тобто вказаний запит не вимагав уточнення діагнозу, методів лікування, а стосувався лише підтвердження перебування працівника на лікуванні у зазначеному закладі охорони здоров`я відповідно до відкритого листка непрацездатності. На вказаний запит уповноваженим представником Другої міської клінічної лікарні надано відповідь за інформацією щодо листка непрацездатності позивача. Так як запит був здійснений ПАТ «Полтаваобленерго», як роботодавцем, щодо листка непрацездатності, наданого працівником (позивачем у справі), факт звернення роботодавця до 2-ої міської клінічної лікарні та період лікування вказаний у листку непрацездатності вже не був

конфіденційною інформацію на момент отримання медичним закладом запиту ПАТ «Полтаваобленерго». Окрім того, позивач при звернені до вказаного медичного закладу, своїм підписом у вкладному листку до облікових форм документації «Інформована добровільна згода пацієнта на обробку персональних даних», надав згоду 2-ій міській клінічній лікарні м. Полтави на обробку своїх персональних даних.

Згідно з листом Міністерства охорони здоров`я від 12.06.2017 р. №3.04.02-Н-7698/6898-зв [180], порядок видачі в медичних закладах документів, що засвідчують тимчасову непрацездатність громадян, визначений Інструкцією №455. Виданий відповідно до цієї Інструкції листок непрацездатності може бути перевірений роботодавцем щодо правомірності його видачі працівнику. Тобто, роботодавець має право перевірити правомірність видачі листка непрацездатності шляхом запиту до структурного підрозділу з питань охорони здоров`я обласної, Київської міської державної адміністрації, у підпорядкуванні якого знаходиться заклад охорони здоров`я, який видавав листок непрацездатності.

Також ПАТ «Полтаваобленерго» було надіслано запит щодо надання інформації стосовно працівника (позивача) на адресу Комунального закладу «Центр первинної медико-санітарної допомоги № 2 м. Полтави». У запиті зазначалося, що в провадженні Ленінського районного суду м. Полтава знаходиться цивільна справа за позовом працівника до ПАТ «Полтаваобленерго» про стягнення моральної шкоди та скасування наказів, у якій позивач посилався на певну інформацію щодо стану свого здоров`я та фактів звернення до медичних закладів для отриманням медичної допомоги та лікування. З метою підтвердження або спростування інформації про звернення до лікувальних закладів та про видачу листків непрацездатності ПАТ «Полтаваобленерго» просило надати відомості. Інформація стосовно працівника запитувались ПАТ «Полтаваобленерго», як стороною у цивільній справі та у зв`язку із відомостями, які стали відомі під час розгляду справи, з метою збирання доказів в обґрунтування своїх вимог та заперечень. У відповідь на цей запит листом КЗ «ЦПМСД №2 міста Полтави» було

повідомлено ПАТ «Полтаваобленерго», що запитувана інформація не буде надана відповідно до ст. 286 ЦК України та ст. 40 Закону України «Основи законодавства України про охорону здоров`я». У запиті ПАТ «Полтаваобленерго» не вимагалось надання інформації про діагноз та методи лікування. В свою чергу, відповідь на запит не містила відомостей про діагноз та методи лікування, а також іншої інформації, яка містить лікарську таємницю.

Отже, судом порушень прав позивача на захист персональних даних, а також права на таємницю про стан здоров`я – не встановлено. Окрім того, судом встановлено, що на адресу Четвертої міської клінічної лікарні міста Полтави надходили запити ПАТ «Полтаваобленерго» аналогічного змісту щодо надання відомостей про видачу працівнику (позивачу) листків непрацездатності. У відповідь на вказані запити (медичним закладом повідомлено про відсутність факту звернення працівника до медичного закладу. Оскільки позивач (працівник) не був пацієнтом Четвертої міської клінічної лікарні міста Полтави, відповідно, вказаний медичний заклад не був володільцем жодної інформації щодо нього, персональних даних останнього, та відомостей, що становлять лікарську таємницю. При цьому у запиті ПАТ «Полтаваобленерго» не вимагалось надання інформації про діагноз та методи лікування, а відповідь на запит не містила і не могла містити відомостей про факти звернення працівника до медичного закладу за медичною допомогою, оскільки такі були відсутні.

Судом також встановлено, що на адресу Комунального закладу «Центр первинної медико-санітарної допомоги №1 м. Полтави» від ПАТ «Полтаваобленерго», як роботодавця, надходили запити щодо звернення та видачі листків непрацездатності працівнику (позивачу) із зазначенням його персональних даних (ПІБ, дати народження, адреси). Цим медичним закладом надано відповіді про відсутність звернень за медичною допомогою директора з правової роботи ПАТ «Полтаваобленерго» – працівника (позивача). У запиті ПАТ «Полтаваобленерго» не вимагалось надання інформації про діагноз та методи лікування, а відповідь на запит, в свою чергу, не містив і не міг містити

відомостей про факти звернення працівника до медичного закладу за медичною допомогою, оскільки такі були відсутні.

Таким чином, з досліджених письмових доказів судом не встановлено порушень права позивача на захист персональних даних, а також права на таємницю про стан здоров`я.

Апеляційний суд погодився із висновками суду 1-ї інстанції щодо того, що здійснені ПАТ «Полтаваобленерго», як роботодавцем, запити відносно працівника із зазначенням його персональних даних, як суб`єкта персональних даних, який не обмежував роботодавця у використанні власних персональних даних, які не виходять за межі встановленої законом заборони, – не суперечать вимогам Закону України «Про захист персональних даних» та не порушили прав позивача на захист персональних даних. Також правильним є висновок суду, що надані медичними закладами, які не були володільцями персональних даних відносно позивача, а відповідно, володільцями інформації, що становить персональні дані та лікарську таємницю відносно нього, у зв`язку з тим, що останній не звертався до них за медичною допомогою взагалі (не був пацієнтом), тому відомості про відсутність факту звернення до медичних установ та видачі позивачу (працівнику) листків непрацездатності, не порушують вимог Закону України «Про захист персональних даних» та Закону України «Основи законодавства України про охорону здоров`я».

Суд дійшов правомірного висновку, що встановлене не свідчить про незаконність дій вищезазначених медичних закладів, які у відповіді на запит повідомили про відсутність факту звернення до медичних установ та видачі позивачу листків непрацездатності. Така надана інформація не є розголошенням відомостей про особу, що становлять лікарську таємницю, а стосується підтвердження факту їх законної видачі медичним закладом на запит роботодавця. А персональні дані позивача (працівника) (ПІБ, дата народження, адреса), що містилися у відповідях медичних установ на запити ПАТ «Полтаваобленерго», безпосередньо були зазначені у самих запитах

роботодавця, і не є, по суті, запитуваною інформацією, а тому не є у такому разі розголошенням медичними установами персональних даних працівника .

За встановлених обставин, суд дійшов правильного висновку про відсутність протиправних дій з боку відповідачів відносно позивача, а саме відсутність порушення права останнього на захист персональних даних та права на таємницю про стан здоров`я. За недоведеності факту протиправності дій відповідачів, обґрунтованим є висновок суду щодо відсутності правових підстав для задоволення позовних вимог і в частині відшкодування моральної шкоди, як похідних, які є безпідставними, а відтак задоволенню не підлягають. Відтак, апеляційну скаргу позивача (працівника) залишили без задоволення [117].

Наведемо ще приклад судової справи про передачу третіми особами таких «чутливих» персональних даних як – стан здоров'я працівника. Так, позивачка в період з 17 листопада 2016 року по 25 квітня 2017 року працювала в Софіївському районному суді Дніпропетровської області на посаді помічника голови Софіївського районного суду Дніпропетровської області та звільнена на підставі п. 2 ст. 36 КЗпП України.

25 квітня 2017 року керівником апарату Софіївського районного суду Дніпропетровської області на адреси Департаменту охорони здоров`я Дніпропетровської обласної ради, Головного лікаря комунального закладу охорони здоров`я «Софіївський районний центр первинної медико-санітарної допомоги» та головного лікаря комунального закладу «Софіївська центральна районна лікарня» Дніпропетровської обласної ради» направлено письмовий запит про термінове повідомлення суду інформації такого змісту: «Чи зверталася до вашого закладу конкретна працівниця (позивачка), якщо так, то до якого лікаря і чи є відкритий лікарняний лист та з якої дати?».

22 травня 2017 року позивачка звернулася зі скаргою до голови Софіївського районного суду Дніпропетровської області, в якій просила прийняти рішення, яке передбачене п. 3 ч. 1 ст. 24 Закону України «Про судоустрій і статус суддів», тобто внести подання про застосування до керівника апарату суду накладення дисциплінарного стягнення відповідно до

законодавства, також на підставі пунктів 7 та 9 ч. 1 ст. 65 Закону України «Про державну службу» встановити з якою метою діяла керівниця апарату суду, направляючи запити щодо стану здоров`я позивачки в установи лікарень, зокрема встановити – чи вбачається в її діях перевищення службових повноважень, якщо воно не містить складу злочину або адміністративного правопорушення; чи використовувала вона свої повноважень в особистих (приватних) інтересах або в неправомірних особистих інтересах інших осіб, та на підставі вищевикладеного притягти керівницю апарату до дисциплінарної відповідальності та інших осіб, які відповідають за збереження персональних даних та причетні до розкриття, використання конфіденційної інформації щодо позивача.

За змістом письмової відповіді від 31 травня 2017 року, голова Софіївського районного суду Дніпропетровської області, зокрема вказала, що у запиті Софіївського районного суду Дніпропетровської області до медичних закладів зазначено дату народження та місце проживання позивачки для того, щоб ідентифікувати особу, так як під таким самим прізвищем, ім`ям та по-батькові можливо є ще одна медична картка на іншу фізичну особу. Порушене питання буде обговорено на зборах апарату Софіївського районного суду Дніпропетровської області. Також головою суду принесені вибачення.

За доводами позивачки керівниця апарату суду безпідставно та протиправно допустила розголошення персональних даних щодо дати народження та місця проживання, які стали відомі їй під час виконання посадових обов`язків, неправомірно збирала інформацію щодо стану здоров`я.

Керівник апарату Софіївського районного суду Дніпропетровської області, вказуючи на відсутність протиправності запиту, зазначала, що позивачем у день та до звільнення телефонограмою передано інформацію про перебування на лікуванні з 24 квітня 2017 року, отримання інформації про перебування чи не перебування позивача у стані тимчасової непрацездатності було обумовлено необхідністю вирішення питання трудових відносин з позивачем, оскільки основний працівник приступив до виконання обов`язків.

Суд першої інстанції виходив з того, що керівник апарату Софіївського районного суду Дніпропетровської області, під час звернення до лікарняних закладів із запитом про надання інформації щодо позивача, зазначивши її персональні дані (адресу та дату народження), діяла всупереч вимогам ст. 32 Конституції України, Закону України «Про інформацію» та Закону України «Про захист персональних даних».

Суд апеляційної інстанції не погодився з висновком суду першої інстанції та, відмовляючи в задоволенні позову зазначив, що персональні дані працівника, які містяться в паспорті або документі, що посвідчує особу, в трудовій книжці, документі про освіту (спеціальність, кваліфікацію), документі про стан здоров`я та інших документах, які працівник подав при укладенні трудового договору, обробляються володільцем бази персональних даних на підставі ст. 24 КЗпП України виключно для здійснення повноважень володільця бази персональних даних у сфері правовідносин, які виникли в нього з працівником на підставі трудового договору (контракту). Відтак, жодних порушень не було допущено.

ВС, дійшов висновку, що керівниця апарату Софіївського районного суду Дніпропетровської області при зверненні до лікарняних закладів із запитом про надання інформації щодо позивачки, зазначивши її персональні дані (адреса та дата народження), діяла всупереч вимогам ст. 32 Конституції України, Закону України «Про інформацію» та Закону України «Про захист персональних даних».

Відтак, ВС погодився з висновком суду першої інстанції про визнання протиправними дій керівниці апарату Софіївського районного суду Дніпропетровської області щодо розголошення персональних даних позивачки, які їй стали відомі під час виконання нею посадових обов`язків.

Таким чином, суд апеляційної інстанції дійшов помилкового висновку, що оскільки керівницею апарату Софіївського районного суду Дніпропетровської області не витребовувалася інформація щодо безпосереднього стану здоров`я або діагнозу можливого захворювання позивачки, спеціалізації лікаря, то під час здійснення запиту до медичних

закладів щодо позивачки діяла в службових інтересах, в межах посадових повноважень та не порушила права та охоронювані законом інтереси позивача в сфері захисту персональних даних [116].

У аналізованих справах погоджуємося із висновками судів. Поряд із цим, наголосимо, що інформація про стан здоров'я працівника належить до категорії «чутливих» персональних даних, тому обробка такої інформації становить особливий ризик для прав і свобод суб'єкта персональних даних. Статтею 7 Закону № 2297 [137] встановлено особливі вимоги до обробки таких персональних даних. Так, обробка цих даних заборонена, окрім вказаного у ч. 2 зазначеної статті вичерпного переліку випадків.

Зауважимо, ані КЗпП України, ані жодним законом України (у т. ч. законодавством про захист персональних даних) не передбачено обов'язку або можливості надання закладом охорони здоров'я або правоохоронним органом відомостей про події або явища, що відбуваються у житті працівника (звернення за медичною допомогою, перебування на лікуванні, участь в досудовому розслідуванні у якості свідка тощо), на запит роботодавця.

Таким чином, відмова офіційних органів у наданні інформації про працівника є цілком правомірною, а від усталеної практики занадто активних «самостійних розшукових дій» роботодавця у разі нез'явлення працівника на роботу слід відмовитися як від такої, що суперечить нормам законодавства у сфері захисту персональних даних.

Важливо підкреслити, що інформація про стан здоров'я працівника буває необхідною роботодавцю для вирішення питання про можливість допуску того чи іншого працівника до виконання певної роботи. У таких випадках потрібно керуватися положеннями Кодексу практики МОП із захисту особистих даних про працівника про те, що у разі медичного обстеження роботодавець повинен бути поінформованим тільки про ті висновки, що стосуються питання про можливість використання працівника; висновки не повинні містити інформацію медичного характеру. Вони можуть, якщо це потрібно, містити вказівки на придатність до певної роботи або характер та

умови роботи, що протипоказані з медичних міркувань на тимчасовій чи постійній основі [175, с. 12].

**Висновки до розділу 2**

Вивчивши сучасний стан та проблеми забезпечення захисту персональних даних працівників в Україні, зроблено такі основні висновки.

1. Із заглибленням процесів цифровізації доцільним убачається закріплення нормативного припису щодо надання працівником інформації за допомогою ІКТ із використанням електронного підпису або кваліфікованого електронного підпису.

2. Надавати інформацію про персональні дані працівника на телефонний запит не можна, позаяк таку інформацію слід надавати тільки за письмовими запитами та за згодою працівника, яку він/вона надав(ла), або володільцю його персональних даних, або запитувачу. Оскільки якщо передавати таку інформацію телефоном, то роботодавець ризикує, адже працівник може поскаржитися омбудсмену на те, що роботодавець незаконно поширив його/її персональні дані, а як наслідок роботодавець може отримати штраф.

3. Наразі законодавство у сфері військового обліку не містить ані обов’язку роботодавця надавати копію наказу про звільнення працівника, ані права ТЦК та СП вимагати його, то роботодавець може відмовляти у наданні ТЦК та СП такої інформації.

4. Надання персональних даних працівників на запити поліції може здійснюватися тільки з чітко визначеними цілями та у конкретних випадках, то надання роботодавцем цих відомостей буде правомірним та не порушуватиме чинне законодавство про захист персональних даних працівників. Теж саме стосується і випадків надання персональних даних працівників на письмовий запит прокуратури. За загальним правилом, роботодавець може надавати такі відомості за згодою працівника. Якщо згоди

немає, то надавати можна якщо в письмовому запиті прокуратури обґрунтовані його мета та (або) правові підстави.

5. Відмова надати інформацію на адвокатський запит, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, є порушенням законодавства та може призвести до притягнення до відповідальності, крім випадків відмови в наданні інформації з обмеженим доступом.

6. Інформація, отримана роботодавцем про особу, котра шукає роботу, повинна бути знищена, як тільки стане зрозуміло, що особі не буде зроблено пропозицію обійняти вакантну посаду або ж особа відмовляється від запропонованої посади.

7. Ані КЗпП України, ані жодним законом України (у т. ч. законодавством про захист персональних даних) не передбачено обов’язку або можливості надання закладом охорони здоров’я або правоохоронним органом відомостей про події або явища, що відбуваються у житті працівника (звернення за медичною допомогою, перебування на лікуванні, участь в досудовому розслідуванні у якості свідка тощо), на запит роботодавця. Тому відмова офіційних органів у наданні інформації про стан здоров’я працівника, про його звернення чи не звернення до медичних закладів, є цілком правомірною. Інформація про стан здоров'я працівника може бути необхідною роботодавцю для вирішення питання про можливість допуску того чи іншого працівника до виконання певної роботи, але у такому випадку цю інформацію роботодавець має отримати виключно від самого працівника.

# РОЗДІЛ 3
# НАПРЯМИ ВДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ В УКРАЇНІ

## 3.1 Гарантії захисту персональних даних працівників в Україні

Гарантії захисту персональних даних є елементом механізму правового регулювання захисту персональних даних працівників. Чинне законодавство передбачає такі гарантії: (1) заборона обробки певних видів персональних даних або спеціальний порядок такої обробки; (2) право працівника на вільний доступ до відомостей про себе, що містяться у роботодавця; (3) створення спеціально уповноваженого органу контролю за дотриманням законодавства про захист персональних даних, яким є обмудсмен; (4) передбачення юридичної відповідальності за порушення законодавства у цій сфері тощо.

На думку І. М. Сопілко, захист персональних даних – це вміння балансувати між інформаційною відкритістю та закритістю, між двома прагненнями: максимально розширити доступ громадян до невтаємниченої публічної інформації (державної, наукової, освітньої, персональної тощо) і, водночас, максимально захистити інформацію приватного змісту [167, с. 69]. Хоча поставлена задача є непростою, передові країни Західної Європи успішно з нею справляються. При удосконаленні національного законодавства у цій сфері доцільно спиратися на їх напрацювання.

Гарантії захисту персональних даних працівника – це система нормативно визначених засобів забезпечення конфіденційності інформації про особу працівника, що поширюється на всі етапи обробки персональних даних (від збирання до знищення), а також неможливості несанкціоноваго доступу до такої інформації третіх осіб.

Залежно від поширення гарантії захисту персональних даних працівників поділяються на загальні (передбачені для всіх фізичних осіб) та спеціальні (пов’язані з правовим статусом працівника).

Як зазначає Р. В. Куценко, до загальних гарантій захисту персональних даних працівників відносяться:

1) встановлення законодавчих вимог та підстав обробки персональних даних працівника. Відповідні умови та підстави визначені статтями 6, 7 та 11 Закону України № 2297 [137]. Основними вимогами до обробки персональних даних визначені такі: обробка має здійснюватися з конкретно та чітко визначеною метою (стосовно персональних даних працівника такою метою може бути перевірка рівня кваліфікації та компетентності працівника, нарахування заробітної плати, сплата податків та зборів до фондів соціального страхування тощо); обробка персональних даних має здійснюватися прозоро та дозволеними засобами; склад та зміст персональних даних мають бути адекватними та сумісними з метою обробки; недопустимість обробки даних про працівника, які є конфіденційними, без його згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [76, с. 158-159];

2) безкоштовний та вільний доступ працівників до своїх персональних даних. Персональні дані працівника, як правило, зберігаються в кадровому відділі, відділі бухгалтерії та ін. Відповідні відділи за зверненням працівника

мають видавати запитувану інформацію у формі виписок, довідок тощо. Будь-які обмеження та заборони щодо надання працівнику інформації, яка складає зміст його персональних даних, мають бути визнані незаконними;

3) функціонування спеціально уповноваженого органу у сфері здійснення контролю за додержанням законодавства про захист персональних даних [103, с. 56]. До спеціальних гарантій у сфері захисту персональних даних працівників належать:

1) під час оформлення трудових правовідносин та виконання трудової функції забороняється обробляти певні види інформації. Згідно зі ст. 7 Закону України № 2297 [137] забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до

кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних;

2) під час збирання роботодавцем додаткової інформації про працівника (з відкритих джерел, соціальних мереж, попередніх місць роботи тощо) обов'язково необхідно отримати письмову згоду працівника;

3) захист роботодавцем персональних даних працівників та заборона несанкціонованого доступу до таких відомостей сторонніх осіб.

Як справедливо відзначають вчені-трудовики, чинне законодавство в недостатній мірі регламентує спеціальні гарантії захисту персональних даних працівників [76, с. 160-161].

Наголосимо, що письмові згоди на обробку персональних даних працівників слід було отримували від працівників до 2014 року. Наразі таку згоду отримувати не треба. Такий виняток визначає ст. 11 Закону № 2297 [137]. Так, згода не потрібна, якщо є необхідність виконання обов'язку володільця персональних даних, який передбачений законом (п. 5 ст. 11 Закону № 2297 [137]). Але так як кожен роботодавець має обов'язок забезпечити реалізацію трудових відносин згідно з КЗпП України, тому слід належно обробляти та захищати персональні дані працівника.

Зауважимо, що не слід плутати згоду працівника із зобов'язанням про нерозголошення. Зобов'язання працівника про нерозголошення персональних даних – обов'язковий документ, який повинен підписати кожен працівник, що має справу з персональними даними інших осіб, адже цей документ вимагатимуть при перевірці.

Наразі дуже актуальним є питання розміщення інформації про працівників на корпоративному сайті підприємства, установи чи організації, а також у соціальних мережах. Звісно, постає питання – а чи отримувати згоду працівника у таких випадках. Загальне правило містить Закон № 2297 [137], яке не вимагає згоди працівника на обробку його персональних даних, якщо роботодавець обробляє персональні дані з метою реалізації трудових відносин. У цьому разі є законна підстава для обробки даних – «необхідність виконання обов'язку володільця персональних даних, який передбачений

законом» (п. 5 ст. 11 Закону № 2297 [137]). Утім, якщо підприємство хоче використовувати відомості щодо працівника як власну конкурентну перевагу, для підвищення ділової репутації, просування товарів чи послуг в Інтернеті, соцмережах, згода на обробку персональних даних потрібна. Наведемо приклад. Приватний медичний центр створив на сайті розділ «Наша команда», де хоче розмістити відомості про лікарів, їх освіту, досвід роботи, спеціалізацію, а також фото.

Відомості щодо подій та явищ, які відбувалися або відбуваються у товариському, професійному, діловому та інших сферах життя особи належать до персональних даних. Виняток – дані щодо виконання повноважень особою, яка займає посаду, пов’язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу є конфіденційною, може бути поширена тільки за її згодою і лише в інтересах національної безпеки, економічного добробуту та прав людини. Винятки – випадки, визначені законом (рішення КСУ від 20.01.2012 р. № 2-рп/2012 [158]).

Отже, приватний медичний центр може розмістити інформацію про лікаря на сайті тільки за його згодою [182].

У таких випадках роботодавцю варто пояснити працівнику, на що він погоджується і з якою метою. Згода суб’єкта на обробку його персональних даних повинна бути добровільною та інформованою (п. 2.8 Типового порядку від 08.01.2014 р. [128]).

Щоби надати згоду, працівник попередньо повинен отримати відповіді на питання:

– хто оброблятиме його персональні дані — вкажіть назву володільця персональних даних, його адресу, контактні телефони тощо;

– з якою метою оброблятимуть персональні дані — формулюйте мету чітко та зрозуміло;

– які персональні дані оброблятимуть — наведіть конкретний вичерпний перелік персональних даних, що плануєте обробляти;

– які дії з персональними даними передбачатиме їх обробка — наприклад, збирання, зберігання, передання, оприлюднення, знеособлення тощо;

– хто є розпорядником персональних даних — завважте права і повноваження розпорядника щодо обробки персональних даних;

– кому можуть бути передані персональні дані, з якою метою, на яких підставах;

– скільки часу персональні дані будуть зберігатися у володільця;

– на яких умовах працівник може відкликати згоду на обробку персональних даних та які наслідки такої дії.

Також доцільно поінформувати щодо інших прав, визначених ст. 8 Закону № 2297 [137] (Роз'яснення до Типового порядку обробки персональних даних Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р.) [163]. Відповіді на означені питання можна надати усно, але ліпше викласти у локальному акті роботодавця, наприклад, у Положенні про обробку та захист персональних даних працівників та контрагентів.

Суб'єкт персональних даних може надавати згоду у письмовій або електронній формі, що дає змогу зробити висновок про її надання (п. 2.8 Типового порядку). Якщо згоду доведеться отримувати періодично від нових працівників, то доречно на практиці розробити трафарет, а у документі визначити, що саме дозволяє обробляти особа і з якою метою.

Згода суб'єкта персональних даних – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди (ст. 2 Закону № 2297 [137]). Обробку персональних даних здійснюють для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством. Заборонена обробка даних про фізичну особу, які є конфіденційною інформацією без її згоди, крім випадків,

визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (п. 5 та 6 ст. 6 Закону № 2297 [137]).

Роботодавцю слід надати працівнику можливість зробити застереження щодо обмеження права на обробку персональних даних під час надання згоди. Це право особи, визначене п. 10 ст. 8 Закону № 2297 [137].

Працівник може відкликати згоду зможе будь-коли. Це його право, закріплене у п. 11 ст. 8 Закону № 2297 [137], при цьому працівник не повинен пояснювати, чому відкликає згоду. Суб'єкт персональних даних має право відкликати згоду на обробку персональних даних без зазначення мотивів, у разі якщо єдиною підставою для обробки є згода суб'єкта персональних даних. З моменту відкликання згоди володілець зобов'язаний припинити обробку персональних даних (п. 2.15 Типового порядку).

Роботодавець повинен визначте, де і скільки зберігатимете згоди працівників. Наприклад, у справах відділу кадрів чи відділу маркетингу, або департаменту з розвитку бізнесу. Зауважимо, що законодавство не скеровує, в якому структурному підрозділі зберігати згоди на обробку персональних даних. Підприємство визначає це на власний розсуд. Володілець персональних даних має зберігати документи (інформацію), які підтверджують, що суб'єкт надав згоду на обробку його персональних даних, впродовж часу обробки таких даних (п. 2.8 Типового порядку [128]). Отже, допоки інформація про працівника є на сайті чи в соцмережах, зберігайте згоду на обробку персональних даних, щоби підтвердити, що дотримуєте Типового порядку.

Якщо згода надана на певний строк, то й інформація про працівника може бути розміщена лише протягом цього строку (п.п. 1 п. 2 ст. 15 Закону № 2297 [137]).

Якщо надалі виникне потреба використовувати персональні дані з іншою метою, несумісною з попередньою, отримайте нову згоду. У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб'єкта персональних даних на обробку його даних

відповідно до зміненої мети, якщо інше не передбачено законом (п. 1 ст. 6 Закону № 2297 [137]).

Нині у час розвитку цифрових технологій, новітніх телекомунікаційних технологій, повсякчас виникає питання щодо допусків працівників на територію підприємства, установи чи організації. Зокрема, наразі актуальним є питання щодо можливості запровадження допуску на підприємство через відбитки пальців.

У цьому контексті зазначимо, що Закон не забороняє запроваджувати допуск працівників на підприємство шляхом обробки відбитків пальців. Але процедура запровадження — вельми клопітка. Доведеться врахувати вимоги законодавства у сфері захисту персональних даних. Адже відбитки пальців належить до персональних біометричних даних. Такі дані вважають особливо чутливими, адже їх обробка становить особливий ризик для прав і свобод людини.

Відтак, Закон дозволяє обробляти біометричні дані, якщо працівник – суб'єкт персональних даних надав на це однозначну згоду (ч. 2 ст. 7 Закону України № 2297 [137]). Тому роботодавець має отримати від кожного працівника згоду на обробку персональних даних у вигляді обробки відбитків пальців. При цьому така згода має бути свідомою – працівник має розуміти, на що погоджується, хто і з якою метою оброблятиме його відбитки пальців, які ризики це спричиняє (ст. 2 Закону № 2297 [137]).

Підкреслимо, що якщо хоча б один працівник не надасть згоду на обробку відбитків пальців, ото запровадити обробку біометричних даних роботодавець не зможе. Однак важливо звернути увагу, що не можна звільнити з ініціативи роботодавця, працівника, який не погоджується на обробку його біометричних даних.

Якщо ж роботодавець отримав згоду на обробку біометричних даних від усіх працівників, то слід:

– визначити наказом відповідального за організацію роботи із захисту персональних даних (ч. 2 ст. 24 Закону № 2297 [137]);

– унести зміни до Положення про порядок обробки і захисту персональних даних працівників;

– направити повідомлення про обробку чутливих даних до Секретаріату Уповноваженого ВР з прав людини.

Підприємство, як володілець персональних даних, має повідомити Уповноваженого ВР з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних. Строк повідомлення — упродовж 30 робочих днів із дня початку такої обробки (ст. 9 Закону № 2297[137]). У ньому доведеться докладно прописати, з якою метою роботодавець обробляє відбитки пальців, а також яких організаційних і технічних заходів ужито, щоби забезпечити захист біометричних даних на підприємстві. Адже за порушення може настати адміністративна відповідальність (ст. 188-39 та ст. 188-40 КУпАП [96]).

**Відповідальність за порушення у сфері захисту персональних даних** [82]

| **Норма законодавства, якою встановлено відповідальність** | **Склад порушення** | **Санкція** | **Норми законодавства, якими встановлено відповідні вимоги** |
|---|---|---|---|
| Частина перша статті 188-39 КпАП | 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 | Штраф: на громадян – від 100 до 200 нмдг на посадових осіб, громадян – суб'єктів підприємницької діяльності – від 200 до 400 нмдг | 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 |

| | | | |
|---|---|---|---|
| | недостовірних відомостей | | дня початку такої обробки... Володілець персональних даних зобов'язаний повідомляти Уповноваженого про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни (п. 1 , п. 3 ст. 9 Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI ) |
| Частина друга статті 188-39 КпАП | 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 | Штраф:<br>на громадян — від 200 до 300 нмдг<br>на посадових осіб, громадян — суб'єктів підприємницької діяльності — від 300 до 1000 нмдг | Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи:<br>1) Уповноважений Верховної Ради з прав людини;<br>2) суди (ст. 22 Закону України «Про захист персональних даних» ) |

| | | | |
|---|---|---|---|
| | | | Уповноважений має такі повноваження у сфері захисту персональних даних…<br>5) за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних (ст. 23 Закону України «Про захист персональних даних» ) |
| Частина третя статті 188-39 КпАП | Повторне протягом року вчинення | Штраф: | |

| | | | |
|---|---|---|---|
| | порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративном у стягненню | на громадян – від 300 до 500 нмдг на посадових осіб, громадян – суб'єктів підприємницько ї діяльності – від 500 до 2000 нмдг | |
| Частина четверта статті 188-39 КпАП | 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 | Штраф: на громадян – від 100 до 500 нмдг; на посадових осіб, громадян – суб'єктів підприємницько ї діяльності – від 300 до 1000 нмдг | 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 (ч. 1 ст. 24 Закону України «Про захист персональних даних» ) |
| Частина п'ята статті 188-39 КпАП | Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано | Штраф від 1000 до 2000 нмдг | |

| | | | |
|---|---|---|---|
| | адміністративном у стягненню | | |
| Стаття 188-40 КпАП | Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини | Штраф на посадових осіб, громадян – суб'єктів підприємницької діяльності від 100 до 200 нмдг | ст. 22, 23 Закону України «Про захист персональних даних» |
| Частина перша статті 182 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 | Штраф від 500 до 1000 нмдг або виправні роботи на строк до 2 років, або арешт на строк до 6 місяців, або обмеження волі на строк до 3 років | 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 (ст. 32 Конституції України ) |
| Частина друга статті 182 Кримінального кодексу України | Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи (істотною шкодою у цій статті, якщо | Арешт на строк від 3 до 6 місяців або обмеження волі на строк від 3 до 5 років, або позбавлення волі на той самий строк | |

| | | | |
|---|---|---|---|
| | вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в 100 і більше разів перевищує нмдг) | | |

### 3.2 Перспективні напрями вдосконалення і розвитку забезпечення захисту персональних даних працівників в Україні

Потреба в удосконаленні положень національного законодавства у сфері захисту персональних даних працівника обумовлена тим, що порушення права працівника на збереження конфіденційності інформації про себе, дотримання мети обробки персональних даних, та вчинення багатьох порушення не тільки мають місце та є досить поширеними у сучасному інформаційному суспільстві, але й у більшості випадків ігноруються як правоохоронними органами, так і самими суб'єктами персональних даних, які не використовують активних засобів щодо захисту своїх прав у відповідній сфері [76, с. 111].

У цьому аспекті також необхідно погодитись з тим, що особливості розвитку правовідносин із збереження особистих прав у процесі застосування персональної інформації на внутрішньодержавному рівні – вагома проблема як минулого, так і сучасного інформаційного періоду. А тому вдосконалення процесу використання персональної інформації має стати предметом наукових досліджень та правового регулювання [100, с. 246].

І. М. Сопілко, одним з проблемних моментів в обробці персональних даних називає їх використання роботодавцем у зв'язку з відсутністю чіткого розуміння складових та видів інформації про особу, які відносяться законодавством до персональних даних працівника [169, с. 941].

Д. В. Цвірюк до основних недоліків законодавства України у сфері захисту персональних даних відносить: неналежне визначення поняття

«персональні дані» в чинному законодавстві; існування розбіжностей у нормативно-правовому закріпленні поняття «персональні дані»; відсутність у законодавстві переліку відомостей, що становлять персональні дані; невключення до переліку персональних даних такої інформації, як відомості про фінансовий стан особи та її банківські рахунки, про права власності особи на рухоме та нерухоме майно; відсутність належного наукового опрацювання сфери захисту персональних даних в Україні [173, с. 62].

Найбільш поширеними причинами виникнення порушень у сфері захисту персональних даних працівників в Україні є:

1) надмірне навантаження на Уповноваженого ВРУ з прав людини та його регіональних представників, що унеможливлює охоплення плановими та позаплановими перевірками основного загалу роботодавців та інших учасників правовідносин, які виникають у сфері обігу персональних даних працівника. Крім того, ситуація ускладнюється ще й тим, що у деяких регіонах держави відсутнє представництво Уповноваженого Верховної Ради України з прав людини, що не дозволяє проводити перевірки у таких регіонах, а також своєчасно реагувати на заяви та звернення громадян-суб'єктів персональних даних;

2) низька обізнаність працівників та осіб, які мають намір працевлаштуватися, щодо своїх прав у сфері обробки персональних даних, що зумовлює низьку активність та правовий нігілізм щодо захисту власних прав;

3) недостатня активність Уповноваженого ВРУ з прав людини стосовно проведення планових перевірок на підприємствах, в установах, організаціях усіх форм власності як володільців персональних даних працівників;

4) безвідповідальність роботодавців як володільців персональних даних щодо дотримання вимог законодавства у сфері обігу та захисту персональних даних працівника, зокрема у відносинах з третіми особами, яким передаються відповідні дані;

5) несформованість достатньої судової практики у сфері захисту персональних даних працівника (крім справ, у яких суб'єктами персональних даних виступають державні службовці або інші посадові особи органу

державної влади чи місцевого самоврядування), передусім, з причини низької активності працівників щодо звернення до суду за захистом своїх прав у відповідній сфері [76, с. 118-119].

На думку деяких науковців, до першочергових напрямів удосконалення законодавства у сфері регулювання обігу та обробки персональних даних, що відповідатиме реаліям розвитку і впровадження інформаційно-комунікаційних технологій у суспільне життя, необхідно віднести такі: 1) удосконалення понятійного апарату Закону України «Про захист персональних даних» з обов'язковим розподілом процесів обігу та обробки персональних даних; 2) запровадження класифікацій персональних даних і баз таких даних; 3) визначення правових режимів обігу й обробки окремих видів персональних даних у різних базах персональних даних; 4) розробку і прийняття Закону України «Про обіг та обробку персональних даних» замість чинного Закону України «Про захист персональних даних» [155, с. 192].

А ось В. О. Волосецький вважає, що в Україні напрямами удосконалення правового регулювання відносин, пов'язаних із захистом персональних даних, з урахуванням передового досвіду та права ЄС, мають стати:

1) запровадження дієвого механізму захисту права людини на власні персональні дані, що полягає, серед іншого, у чіткому визначенні об'єктів законодавчого захисту та чітких правових норм, які дозволяють комплексно і системно захищати права суб'єктів персональних даних;

2) запровадження законодавчого механізму встановлення балансу між правом на свободу інформації та правом на захист персональних даних;

3) удосконалення загальних та особливих вимог до обробки персональних даних;

4) уточнення переліку прав суб'єктів персональних даних з урахуванням європейського підходу до визначення абсолютного права на виправлення та видалення власних персональних даних – «права бути забутим»;

5) уточнення процедур обробки персональних даних (збирання, накопичення, зберігання, зміна, доповнення, поновлення, повідомлення,

поширення (розповсюдження, передача), знеособлення, видалення, знищення персональних даних) з урахуванням вимог права ЄС тощо [83, с. 8].

Не можна не погодитися із наведеними позиціями науковців, звісно, належне правове регулювання може забезпечити захист даних, однак і самі суб'єкти мають забезпечувати схоронність даних, тому саме локальне регулювання в аспекті захисту персональних даних має сприяти дієвому захисту персональних даних персоналу. У цьому контексті, А. М. Чернобай наголошує на необхідності прийняття локального нормативно-правового акту, в якому слід закріпити вимоги до обробки персональних даних працівника з урахуванням особливостей та видів діяльності конкретної організації, норми якого не повинні погіршувати становище працівника порівняно з законодавством України про працю [175, с. 11]. Підтримуємо цю позицію і пропонуємо авторський проєкт такого локального документу (Додаток А).

На практиці оформлення ознайомлення працівника з локальним нормативним правовим актом, що визначає порядок обробки персональних даних, здійснюється різними методами. Зазвичай ведеться спеціальний журнал, у якому прийнятий працівник після ознайомлення з локальним нормативним правовим актом ставить свій підпис. У деяких організаціях відмітка про ознайомлення працівника з умовами колективного договору, правилами внутрішнього трудового розпорядку та положенням про захист персональних даних визначається у трудовому договорі.

Локальні нормативні правові акти, що містять норми про використання та захист персональних даних працівника, за суб'єктним критерієм можна класифікувати на акти загального та спеціального характеру. Локальні нормативні правові акти загального характеру поширюються на всіх або більшість працівників організації, а під дію спеціальних актів підпадають певні категорії посадових осіб. До актів загального характеру належать, наприклад, колективний договір, правила внутрішнього трудового розпорядку, положення про підрозділ організації. Спеціальними локальними правовими актами є інструкція з діловодства, положення про захист інформації, положення про персонал організації, посадові інструкції та ін.

У своїй діяльності роботодавець використовує документи двох видів. Першу групу документованої інформації надає працівник під час укладення трудового договору Документи другої групи роботодавець формує самостійно – це первинна облікова документація щодо обліку кадрів. До них належать накази (розпорядження) про прийом, переміщення працівника, про припинення трудового договору, заохочення працівника, особова картка працівника, а також документи щодо розрахунків із оплати праці. Крім відомостей, що дублюють дані із першої групи документів, вони містять інформацію про стаж роботи, дати прийому на роботу та переведень на іншу роботу, переміщень в інший структурний підрозділ, рішення атестаційної комісії, про підвищення кваліфікації, професійну перепідготовку, заохочення та нагороди працівника, строки та види відпусток, соціальні пільги, на які працівник має право та інші дані.

Право працівника на отримання повної інформації про свої персональні дані пов'язані з іншим правом – на вільний безкоштовний доступ до своїх персональних даних, включаючи право на отримання копій будь-якого запису, що містить його персональні дані.

Працівник має право на визначення свого представника для захисту своїх персональних даних, при цьому передача персональних даних представнику працівника обмежується тільки тими відомостями, які необхідні йому для виконання своїх функцій. Роботодавцю забороняється вимагати інформацію про стан здоров'я працівника, якщо вона не належить до питання можливості виконання працівником трудової функції. Працівник має право на доступ до медичних даних, що стосуються виключно його особи.

Велике значення має право працівника вимагати виключення чи виправлення некоректних або неповних персональних даних, а також даних, зібраних із порушенням вимог КЗпП України. За наявності розбіжностей щодо персональних даних оціночного характеру працівник має право доповнити відомості окремою заявою, що виражає його точку зору.

Обробка персональних даних працівника здійснюється роботодавцем з метою сприяння йому у працевлаштуванні, навчанні та просуванні по службі,

забезпечення особистої безпеки, контролю за кількістю та якістю виконуваної роботи та забезпечення схоронності майна роботодавця. Перелік цілей обробки персональних даних має бути закритим і не підлягати розширювальному тлумаченню. Роботодавцю має бути заборонено повідомляти персональні дані працівника в комерційних цілях без письмової згоди.

Всі персональні дані про працівника слід отримувати, перш за все, у нього самого. Оскільки працівник надає інформацію лише про себе, а роботодавець її використовує, то обов'язок несення витрат для забезпечення захисту таких даних лежить на роботодавцеві.

Трудове законодавство також не регулює застосування засобів перевірки чесності, сумлінності працівників, надання достовірності інформації, зокрема через використання поліграфів. Хоча, як зазначається у науковій трудо-правовій літературі, вже доволі часто в Україні використовується поліграф, зокрема, в трьох випадках: при відборі кандидатів для заміщення вакантних посад (кадрового «скринінгу»), під час спеціальних (внутрішніх) перевірок та службових розслідувань, а також при виконанні завдань у межах досудового та судового провадження щодо вчинених кримінальних правопорушень [104, с. 144]. Тому доцільно закріпити добровільність проходження працівником перевірки на поліграфі та заборону застосування такого заходу у випадку відмови від проходження такої перевірки. Її необхідною умовою має бути проведення спеціального розслідування, пов'язаного із нанесенням організації або її працівникам дійсних майнових збитків, а також наявність обґрунтованих підозр про причетність конкретного працівника до певного кримінального правопорушення. Перевірка на поліграфі має здійснюватися на конфіденційній основі та проходити без її демонстрації співробітникам працівника. Вважаємо, що слід закріпити низку медичних протипоказань до проходження тестування.

Одним із напрямів удосконалення законодавства у сфері захисту персональних даних працівника має стати їх зберігання та обробка у інформаційно-комунікаційних системах та мережі Інтернет. Цей напрямок

розвитку вітчизняного законодавства набуває особливої актуальності в сучасних умовах, коли більшість шукачів розміщують своє резюме на веб-сайтах, інших Інтернет-ресурсах, відповідно, роботодавці все частіше звертаються до таких ресурсів з метою здійснення кадрового добору [76, с. 124-125].

Відомості, що містяться в інформаційних базах персональних даних роботодавця, отримані з використанням інформаційно-телекомунікаційної мережі «Інтернет» для встановлення особи працівника та претендента, можуть оброблятися тільки за наявності згоди суб'єкта персональних даних. При прийнятті рішень, які торкаються інтересів працівника, роботодавець не може керуватися лише персональними даними про нього, які отримані виключно внаслідок автоматизованої обробки або електронного одержання.

Особливості роботи з автоматизованою базою персональних даних як набору даних, що ідентифікують працівника та кандидата на посаду, до яких застосовується автоматична обробка: роботодавець зобов'язаний забезпечити цільову відповідність, точність отримання та обробки даних, захист від несанкціонованого використання, посилений режим охорони особливих категорій відомостей (про національну приналежність, погляди та переконаннях, здоров'я та інтимного життя, судимості та ін.).

ATS (*Applicant tracking system*) — це програмне забезпечення, яке дозволяє працювати з кадровими процесами в компанії в електронному вигляді. Такі автоматизовані системи пропонують численні переваги малому та середньому бізнесу, роблячи їхні завдання з підбору та найму персоналу набагато ефективнішими. Не дивно, що програмне забезпечення ATS стає все більш популярним, і все більше компаній розуміють, наскільки легко можна найняти працівників та вести увесь перебіг трудових відносин за допомогою правильного програмного забезпечення.

Звісно, вибір правильної платформи все ще викликає багато труднощів, адже всі організації різні та мають свої власні складності, однак знання ключових характеристик і завчасне визначення конкретних вимог роблять вибір ATS набагато менш громіздким.

Такі автоматизовані системи можуть роботодавцю допомогти здійснити:

– настроюваний конвеєр найму;

– блок-схема найму;

– відстеження ключових показників ефективності (KPI);

– сповіщення про етап найму;

– проведення оцінки кандидатів;

– проведення тестувань кандидатів та працівників;

– перевірка репутації;

– перевірка кандидатів, зокрема оцінка поведінки та когнітивних здібностей кандидата, попередня перевірка кандидатів, перевірка рекомендацій кандидата, тощо.

Використання ATS можу стати у нагоді для перевірки кандидатів на основі кваліфікації для відкритої ролі. Раннє визначення певних якостей кандидата може допомогти підвищити відповідність працівника певній посаді та корпоративній культурі.

Деякі платформи ATS надають швидкі можливості додатків, як-от: автоматичне заповнення полів, функції перетягування для завантаження резюме та супровідних листів, а також чат-боти, автоматичні сповіщення для кандидатів, форму заявки кандидата, портал кандидатів, створення та налаштування шаблонів вакансій, відеопублікація, створена працівниками для рекламних цілей.

ATS також забезпечує кращий зв’язок із кандидатами на посаду протягом усього процесу найму, так і з усіма співробітниками. Нещодавнє дослідження досвіду кандидатів, проведене *CareerBuilder*, показало, що найбільше розчарування для 52% шукачів роботи – це відсутність реакції з боку роботодавців [43]. Тому, використовуючи ATS, можна інформувати кандидатів і відстежувати їхній статус у процесі найму, провадити відеоконференції, здійснювати електронну розсилку та ін.

Такі можливості вимагають надійної системи захисту персональних даних працівників. Але і це автоматизована система надає, оскільки є програмним забезпеченням із високим ступенем кібербезпеки.

Таким чином, автоматизовані системи управління персоналом мають низку переваг, зокрема: мобільність, відповідність даних, візуалізація даних, формування бази кандидатів та співробітників та високий ступінь захисту інформації.

З відносинами з автоматизованої обробки персональних даних пов'язане спостереження за працівником на робочому місці, прослуховування його телефонних розмов та здійснення нагляду в інших формах. Приховане чи явне спостереження працівниками є поширеною практикою, яку здійснюють вітчизняні роботодавці. Однак брак правових норм у цій сфері нерідко призводить до обмеження та порушення прав та законних інтересів працівників.

Слід закріпити, що спостереження за працівником можливе лише у випадках, необхідних для забезпечення збереження майна роботодавцю, усунення загроз здоров'ю та суспільної безпеки. Якщо працівник піддається спостереженню на робочому місці, то він має бути попередньо поінформований про причини спостереження, режим часу спостереження, використовувані методи та засоби збору інформації. Разом з цим, персональні дані, отримані внаслідок спостереження за працівником, не повинні бути єдиною підставою для висновку про продуктивність та якість праці працівника. Роботодавець повинен вжити всі можливі заходи для того, щоб звести до мінімуму «вторгнення» в особисте життя працівника.

Якщо обов'язки роботодавця полягають у цільовому використанні та забезпеченні безпеки відомостей про працівника, то обов'язки працівника зводяться до надання достовірної інформації й її регулярного оновлення. За порушення обов'язків з надання достовірних відомостей роботодавцю повинне бути надане право розірвати трудового договору з власної ініціативи.

**Висновки до розділу 3**

Осмисливши напрямки удосконалення правового регулювання захисту персональних даних працівників, ми зробили такі висновки.

1. Гарантії захисту персональних даних працівника – це сукупність визначених засобів забезпечення конфіденційності інформації про особу працівника, що поширюється на всі етапи обробки персональних даних (від збирання до знищення), а також неможливості несанкціоноваго доступу до такої інформації третіх осіб.

2. Залежно від поширення гарантії захисту персональних даних працівників поділяються на загальні (передбачені для всіх фізичних осіб) та спеціальні (пов'язані з правовим статусом працівника).

3. Згода працівника на оброку персональних даних та зобов'язання про нерозголошення – це не тотожні категорії. Зобов'язання працівника про нерозголошення персональних даних — обов'язковий документ, який повинен підписати кожен працівник, що має справу з персональними даними інших осіб, адже цей документ вимагатимуть при перевірці. А ось згода працівника про оброку його/її персональних даних, за загальним правилом, не є обов'язковою, за винятком «чутливих» даних.

4. У випадку розміщення інформації про працівників на корпоративному сайті підприємства, установи чи організації, а також у соціальних мережах, то роботодавець повинен отримати згоду працівника та визначити, де і скільки зберігатимете згоди працівників. Допоки інформація про працівника є на сайті чи в соцмережах, то слід зберігати згоду на обробку персональних даних. Якщо підприємство хоче використовувати відомості щодо працівника як власну конкурентну перевагу, для підвищення ділової репутації, просування товарів чи послуг в інтернеті, соцмережах, то згода на обробку персональних даних також потрібна.

5. Чинне законодавство не забороняє запроваджувати допуск працівників на підприємство шляхом обробки відбитків пальців, але процедура запровадження — вельми клопітка. Слід врахувати вимоги законодавства у сфері захисту персональних даних, адже відбитки пальців належить до персональних біометричних даних. Такі дані вважають особливо чутливими, адже їх обробка становить особливий ризик для прав і свобод людини. Тому роботодавець має отримати від кожного працівника згоду на

обробку персональних даних у вигляді обробки відбитків пальців. Якщо хоча б один працівник не надасть згоду на обробку відбитків пальців, то запровадити обробку біометричних даних роботодавець не зможе.

6. Особливості роботи з автоматизованою базою персональних даних як набору даних, що ідентифікують працівника та кандидата на посаду, до яких застосовується автоматична обробка: роботодавець зобов'язаний забезпечити цільову відповідність, точність отримання та обробки даних, захист від несанкціонованого використання, посилений режим охорони особливих категорій відомостей (про національну приналежність, погляди та переконаннях, здоров'я та інтимного життя, судимості та ін.).

7. ATS (*Applicant tracking system*) — це програмне забезпечення, яке дозволяє працювати з кадровими процесами в компанії в електронному вигляді. Такі автоматизовані системи пропонують численні переваги малому та середньому бізнесу, роблячи їхні завдання з підбору та найму персоналу набагато ефективнішими. Вибір правильної платформи все ще викликає багато труднощів, адже всі організації різні та мають свої власні складності, однак знання ключових характеристик і завчасне визначення конкретних вимог роблять вибір ATS набагато менш громіздким. Автоматизовані системи управління персоналом мають низку переваг, зокрема: мобільність, відповідність даних, візуалізація даних, формування бази кандидатів та співробітників та високий ступінь захисту інформації.

8. З відносинами з автоматизованої обробки персональних даних пов'язане спостереження за працівником на робочому місці, прослуховування його телефонних розмов та здійснення нагляду в інших формах. Приховане чи явне спостереження працівниками є поширеною практикою, яку здійснюють вітчизняні роботодавці. Однак брак правових норм у цій сфері нерідко призводить до обмеження та порушення прав та законних інтересів працівників. Слід закріпити, що спостереження за працівником можливе лише у випадках, необхідних для забезпечення збереження майна роботодавцю, усунення загроз здоров'ю та суспільної безпеки. Якщо працівник піддається спостереженню на робочому місці, то він має бути попередньо

поінформований про причини спостереження, режим часу спостереження, використовувані методи та засоби збору інформації. Разом з цим, персональні дані, отримані внаслідок спостереження за працівником, не повинні бути єдиною підставою для висновку про продуктивність та якість праці працівника. Роботодавець повинен вжити всі можливі заходи для того, щоб звести до мінімуму «вторгнення» в особисте життя працівника.

# ВИСНОВКИ

На підставі проведеного дослідження трудо-правових аспектів захисту персональних даних працівників, осмислення міжнародного та зарубіжного досвіду, аналізу судової практики щодо збору та обробки персональних даних працівників було з’ясовано особливості захисту персональних даних працівників, а також сформулювано висновки, пропозиції та рекомендації, спрямовані на вдосконалення правового регулювання захисту персональних даних працівників. Основними з них є такі, як-от:

1. Захист персональних даних працівника є елементом трудових правовідносин, а також з метою забезпечення їх одноманітного правового режиму, захист персональних даних працівника слід розглядати як самостійний інститут трудового права. Адже суспільні відносини, пов'язані із захистом персональних даних працівника, є окремими видами правовідносин у сфері праці, які можуть як передувати (надання інформації в ході працевлаштування у певного роботодавця), супроводжувати (приміром, ухвалення рішення про просуванні працівника по службі), так і випливати з трудових правовідносин (приміром, розголошення комерційної таємниці), специфіка яких пов'язана з ключовими суб'єктами трудового права – працівниками та роботодавцями.

2. Інформація про заробітну плату, премії, матеріальну допомогу, будь-які інші виплати з державного чи місцевого бюджету працівнику державного органу або органу місцевого самоврядування не є конфіденційною, не може бути обмежена в доступі та підлягає наданню на запит.

3. Персональні дані працівника – це інформація, яка стосується загальних даних про особу працівника та/або кандидата на посаду, професійної кваліфікації працівника/кандидата на посаду, ділових, професійних якостей, а також інформація щодо спеціальних вимог, які можуть встановлюватися законодавством до працівників/кандидатів на посаду у зв'язку з характером їх роботи (приміром, заповнення декларації про доходи, проходження спеціальної перевірки тощо). Тобто персональні дані працівника мають забезпечувати ідентифікацію його/її не тільки і не стільки як людину, а

насамперед як працівника. Це означає, що персональні дані працівника та претендента на посаду – це, в першу чергу, інформація, що стосується професійної кваліфікації, ділових, професійних якостей та відповідності працівника та претендента на посаду вимогам, які можуть бути до нього пред'явлені у зв'язку з характером роботи.

4. Класифікація персональних даних працівника, в аспекті їх збору, обробки та правового режиму використання має провадитися на такі групи:

а) загальні «анкетні» персональні дані (відомості про прізвище, ім’я, по батькові, дата та місце народження, паспортні дані, відомості про освіту, про професійні навички, відомості про «історію» трудової діяльності тощо);

б) спеціальні персональні дані: расова, національна приналежність, політичні погляди, релігійні чи філософські переконання, стан здоров'я, приватне життя. Збір та обробка цих персональних даних має бути заборонена для роботодавця;

в) персональні дані обмеженого доступу, до яких слід віднести відомості про усиновлення, судимість, участі у кримінальному судочинстві як підозрюваного, наданої чи прийнятої фінансової допомоги, чи послуг, декларація про доходи, результати спеціальної перевірки тощо;

г) біометричні персональні дані – відомості, що містять характеристики фізіологічних та біологічних особливостей людини, що дають можливість встановлення її особистості. Ці дані є «чутливими даними» і мають особливий правовий режим захисту. Для їх обробки роботодавцем потрібне спеціальне погодження Уповноваженим ВРУ.

5. Роботодавець не має права знищувати документи з персональними даними працівника (особову картку П-2 чи документи особової справи). У працівника як суб’єкта персональних даних є право вмотивованої вимоги знищити персональні дані. Однак, право виникає лише тоді, коли дані обробляються незаконно чи є недостовірними.

6. Специфіка захисту персональних даних осіб, які здійснюють свою професійну діяльність на підставі трудового договору, проявляється, перш за все, в тому, що основні вимоги щодо обробки персональних даних працівника

встановлюються нормами законодавства, а порядок здійснення окремих операцій з персональними даними працівника (збір, зберігання, використання, поширення) може деталізуватися у локальних правових актах. Обов'язок не розголошувати персональні дані також може бути передбачений законами та підзаконними актами для окремих категорій осіб, наприклад, для державних службовців.

7. Виокремлено чотири кроки, щоб захистити персональні дані працівника на підприємстві:

а) визначити технічні та організаційні заходи, які треба вжити;

б) призначити відповідального за обробку і захист персональних даних. Якщо роботодавець – орган влади, ОМС чи підприємство, що обробляє чутливі персональні дані, призначайте відповідального обов’язкового. В інших випадках – за рішенням керівника підприємства;

в) розробити Положення про порядок обробки та захисту персональних даних (Додаток А);

г) отримати зобов’язання про нерозголошення персональних даних від працівників, які стикаються під час роботи з персональними даними інших осіб. Зареєструвати отримані зобов’язання в Журналі реєстрації зобов’язань про нерозголошення персональних даних.

8. Із заглибленням процесів цифровізації доцільним убачається закріплення нормативного припису щодо надання працівником інформації за допомогою ІКТ із використанням електронного підпису або кваліфікованого електронного підпису.

9. Надання інформації про персональні дані працівника на телефонний запит неправомірно, позаяк таку інформацію слід надавати тільки за письмовими запитами та за згодою працівника, яку він/вона надав(ла), або володільцю його персональних даних, або запитувачу. Оскільки якщо передавати таку інформацію телефоном, то роботодавець ризикує, адже працівник може поскаржитися омбудсмену на те, що роботодавець незаконно поширив його/її персональні дані, а як наслідок роботодавець може отримати штраф.

10. Ані КЗпП України, ані жодним законом України (у т. ч. законодавством про захист персональних даних) не передбачено обов’язку або можливості надання закладом охорони здоров’я або правоохоронним органом відомостей про події або явища, що відбуваються у житті працівника (звернення за медичною допомогою, перебування на лікуванні, участь в досудовому розслідуванні у якості свідка тощо), на запит роботодавця. Тому відмова офіційних органів у наданні інформації про стан здоров’я працівника, про його звернення чи не звернення до медичних закладів, є цілком правомірною. Інформація про стан здоров'я працівника може бути необхідною роботодавцю для вирішення питання про можливість допуску того чи іншого працівника до виконання певної роботи, але у такому випадку цю інформацію роботодавець має отримати виключно від самого працівника.

11. У випадку розміщення інформації про працівників на корпоративному сайті підприємства, установи чи організації, а також у соціальних мережах, то роботодавець повинен отримати згоду працівника та визначити, де і скільки зберігатимете згоди працівників. Допоки інформація про працівника є на сайті чи в соцмережах, то слід зберігати згоду на обробку персональних даних. Якщо підприємство хоче використовувати відомості щодо працівника як власну конкурентну перевагу, для підвищення ділової репутації, просування товарів чи послуг в інтернеті, соцмережах, то згода на обробку персональних даних також потрібна.

12. Чинне законодавство не забороняє запроваджувати допуск працівників на підприємство шляхом обробки відбитків пальців, але процедура запровадження — вельми клопітка. Слід врахувати вимоги законодавства у сфері захисту персональних даних, адже відбитки пальців належить до персональних біометричних даних. Такі дані вважають особливо чутливими, адже їх обробка становить особливий ризик для прав і свобод людини. Тому роботодавець має отримати від кожного працівника згоду на обробку персональних даних у вигляді обробки відбитків пальців. Якщо хоча б один працівник не надасть згоду на обробку відбитків пальців, то запровадити обробку біометричних даних роботодавець не зможе.

13. Особливості роботи з автоматизованою базою персональних даних як набору даних, що ідентифікують працівника та кандидата на посаду, до яких застосовується автоматична обробка: роботодавець зобов'язаний забезпечити цільову відповідність, точність отримання та обробки даних, захист від несанкціонованого використання, посилений режим охорони особливих категорій відомостей (про національну приналежність, погляди та переконаннях, здоров'я та інтимного життя, судимості та ін.).

14. ATS (*Applicant tracking system*) — це програмне забезпечення, яке дозволяє працювати з кадровими процесами в компанії в електронному вигляді. Такі автоматизовані системи пропонують численні переваги малому та середньому бізнесу, роблячи їхні завдання з підбору та найму персоналу набагато ефективнішими. Вибір правильної платформи все ще викликає багато труднощів, адже всі організації різні та мають свої власні складності, однак знання ключових характеристик і завчасне визначення конкретних вимог роблять вибір ATS набагато менш громіздким. Автоматизовані системи управління персоналом мають низку переваг, зокрема: мобільність, відповідність даних, візуалізація даних, формування бази кандидатів та співробітників та високий ступінь захисту інформації.

15. Із відносинами з автоматизованої обробки персональних даних пов'язане спостереження за працівником на робочому місці, прослуховування його телефонних розмов та здійснення нагляду в інших формах. Приховане чи явне спостереження працівниками є поширеною практикою, яку здійснюють вітчизняні роботодавці. Однак брак правових норм у цій сфері нерідко призводить до обмеження та порушення прав та законних інтересів працівників. Слід закріпити, що спостереження за працівником можливе лише у випадках, необхідних для забезпечення збереження майна роботодавцю, усунення загроз здоров'ю та суспільної безпеки. Якщо працівник піддається спостереженню на робочому місці, то він має бути попередньо поінформований про причини спостереження, режим часу спостереження, використовувані методи та засоби збору інформації. Разом з цим, персональні дані, отримані внаслідок спостереження за працівником, не повинні бути

єдиною підставою для висновку про продуктивність та якість праці працівника. Роботодавець повинен вжити всі можливі заходи для того, щоб звести до мінімуму «вторгнення» в особисте життя працівника.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 2000:477, into force 1.10. 2001, an unofficial translation (Ministry of Labour. URL: www.finlex.fi/pdf/saadkaan/E0010477.PDF

2. Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1. URL: https://edps.europa.eu/data-protection/our-work/publications/legislation/regulation-ec-no-452001_en

3. A list of countries. URL: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-1

4. Abbo Junker. Individualwille, Kollektivgewalt und Staatsintervention im Arbeitsrecht. *NZA.* 1997. P. 1305.

5. Achim Seifert. Bundesdatenschutzgesetz (7th ed. 2011). In: Spiros Simitis (ed.).

6. Act 31 of 8th November 1995 on PREVENTION OF OCCUPATIONAL RISKS, published 10th November 1995 coming into force February 1996. *Official State Gazette (BOE)* on Friday 10th November 1995. BOE Number 269.

7. Act n 78-17 of January 6, 1978 on Information technology, Data files and civil liberties. URL: https://fra.europa.eu/en/law-reference/act-ndeg78-17-6-january-1978-data-processing-data-files-and-individual-liberties

8. Act on Protection of Privacy in Working Life adopted. URL: http://www.eurofound.europa.eu/eiro/2001/06/feature/fi0106191f.htm

9. Act on USE of Health data in the Labour Market (1996). URL: https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=47513

10. Alasdair Maclean. The doctrine of informed consent: does it exist and has it crossed the Atlantic? *Legal Studies (LS).* 2004. Vol. 24. P. 386.

11. Antonio Freni, & Gino Giugni. Lo statuto dei lavoratori. Giuffrè, 1971. 223 p. URL: https://www.maremagnum.com/libri-antichi/lo-statuto-dei-lavoratori/163242755

12. BAG, 15 November 2012, case 6 AZR 339/11.

13. BAG, 20 June 2013, case 2 AZR 546/12.

14. BAG, 21 June 2012, case 2 AZR 153/11.

15. BAG, 21 November 2013, case 2 AZR 797/11.

16. BAG, 27 March 2003, case 2 AZR 51/02.

17. BAG, 27 May 1986, case 1 ABR 48/84.

18. BAG, 30 August 1995, case 1 ABR 4/95.

19. BAG, 6 February 2003, case 2 AZR 621/01

20. BAG, 6 September 2012, case 2 AZR 270/11.

21. BAG, 9 July 2013, case 1 ABR 2/13 (A).

22. C. Bloud-Rey. Quelle place pour l action de la CNIL et du juge judiciaire dans le système de protection des données personnelles? *Recueil Dalloz.* 2013. P. 2795–2801.

23. Civil Code: Act n 70-643 of July 17, 1970. URL: https://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Codigo-Civil-Frances-French-Civil-Code-english-version.pdf

24. CJEU, 16 December 2008, case C-524/06, paras. 51 f. (Huber v Germany).

25. CJEU, 21 November 2001, case C-414/99 (Zino Davidoff SA v A&G Imports Ltd). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A61999CJ0414

26. CJEU, 24 November 2011, case C-468/10 (ASNEF).

27. CJEU, 6 November 2003, case C-101/01, paras. 96 f. (Lindqvist).

28. Conseil Constitutionnel, July 23, 1999, decision n 1999-416. URL: https://www.conseil-constitutionnel.fr/decision/1999/99416DC.htm

29. Conseil Constitutionnel, July 29, 2004, decision n 2004-499. URL: https://www.conseil-constitutionnel.fr/decision/2004/2004499DC.htm

30. Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981. URL: https://www.coe.int/en/web/data-protection/convention108-and-protocol

31. Criminal Code. URL: https://sherloc.unodc.org/cld/en/legislation/tur/criminal_code/second_volume_-_third_chapter_/article_226/article_226.html?.

32. ECHR, 9 April 1997, case 29107/95, (Stedman v UK); cf. Rosemary Jay, Data Protection Law and Practice (3rd ed., 2007). P. 152.

33. F. Douglas Scotti. Il Dialogo Diretto tra L'azienda e il Singolo Lavoratore, in STRATEGIE DI COMUNICAZIONE E STATUTO DEI LAVORATORI (P. Ichino ed., 1992)

34. Frank Hendrickx. Protection of workers' personal data in the European Union. July 2002. 121 p.

35. GDPR. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12002E249:EN:HTML

36. Gerrit Forst. Verarbeitung personenbezogener Daten in der internationalen Unternehmensgruppe. *Der Konzern*. 2012. P. 170–185.

37. Gregor Thüsing. Arbeitnehmerdatenschutz und Compliance (2010).

38. Higher Administrative Court of Hessen (Verwaltungsgerichtshof, VGH), 19 May 2009, case 6 A 2672/08.Z.

39. Higher Labor Court (Landesarbeitsgericht, LAG) of Berlin and Brandenburg, 16 February 2011, case 4 Sa 2132/10.

40. International Covenant on Civil and Political Rights of November 16, 1966. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

41. Josephine Shaw. Informed consent: a German lesson. *International and Comparative Law Quarterly (ICLQ).* 1986. Vol. 35. P. 864.

42. Judgment of the First Senate of 14 July 1999, case 1 BvR 2226/94. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/07/rs19990714_1bvr222694en.html

43. Key ATS (Applicant Tracking System) Requirements and Features. URL: https://www.selecthub.com/hris/ats/applicant-tracking-system-requirements-features/

44. Labor Code. URL: https://www.ilo.org/dyn/travail/docs/2557/Labour%20Code.pdf

45. LAG Hamm, 10 July 2012, case 14 Sa 1711/10.

46. Les libertés publiques et l emploi, rapport pour le ministre du Travail, de l'Emploi et de la Formation professionnelle, dir. G. LYON-CAEN, La documentation française, 1992.

47. Lord Wedderburn, Labour law 2008: 40 years on. *International Law Journal.* 2007. Vol. 36. P. 39.

48. Martin Kock, Julia Francke. Neue Zeitschrift für Arbeitsrecht (NZA). 2009. P. 646, 648.

49. Mykhailyk A. S. International legal standards in the field of protection of personal data of employees. *The scientific heritage.* 2022. N 95(95). P. 35–38.

50. Ogriseg C. GDPR and Personal Data Protection in the Employment Context. *Labour and Law Issues.* 2017. Vol. 3. № 2. 24 p.

51. Opinion 01/2012 on the data protection reform proposals (adopted on 23 March 2012). URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

52. Opinion 2/2017 on data processing at work. Adopted on 8 June 2017. 24 p. URL: https://legalict.com/content/uploads/sites/2/2017/07/Opinion22017ondataprocessingatwork-wp249-2.pdf

53. Opinion 8/2001 on the processing of personal data in the employment contex. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014). P. 23.

54. Otto Kahn-Freund. Labour and the Law. 1972. P. 7.

55. Peter Gola, Rudolf Schomerus. Bundesdatenschutzgesetz (10th ed. 2010).

56. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final. URL: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

57. Protection of Employees Personal Information and Privacy: 2014 JILPT Comparative Labor Law Seminar. *JILPT REPORT.* 2014. No. 14. The Japan Institute for Labour Policy and Training. 226 p.

58. R. De Quenaudon. La cote mal taillée du salarié correspondant à la protection des données à caractère personnel. *Revue droit du travail*. 2006. P. 32.

59. Rapport de la Commission informatique et liberté, dir. B. TRICOT and P. CATALA, La documentation française, 1975. URL: https://www.cnil.fr/sites/default/files/atoms/files/rapport_tricot_1975_vd.pdf

60. Rapport Veil sur le préambule de la Constitution, La documentation française, 2008. URL: https://www.vie-publique.fr/rapport/30242-redecouvrir-le-preambule-de-la-constitution-rapport-du-comite-preside

61. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment: Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies. URL: https://www.apda.ad/system/files/cm-rec-2015-5-en.pdf

62. Recommendation № R (89)2 of the Committee of Ministers to member states on the protection of personal data used for employment purposes: Adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies. URL: https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf

63. Regulation (EU) 2016/679 (General Data Protection Regulation). URL: https://gdpr-info.eu

64. Rosemary Jay. Data Protection Law and Practice (3rd ed.). 2007. P. 152.

65. Royal Legislative Decree 1/1995, of 24th march (BOE of 28th march). URL: https://www.global-regulation.com/translation/spain/1462699/royal-legislative-decree-1-1995-of-24-march%252c-which-approves-the-revised-text-of-the-law-of-the-statute-of-workers.html

66. Rules for the protection of personal data inside and outside the EU. URL: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

67. Section 32l of the bill proposal (24.08.2010). URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.pdf?__blob=publicationFile (as at April 14th, 2014).

68. Seminal Bundesarbeitsgericht (Federal Labour Court, BAG), 5 December 1957, case 1 AZR 594/56.

69. Several articles concerning processing of data in recruitment, Chapter V of Code du Travail, *Journal Officiel* 1.1.1993.

70. Statuto dei Lavoratori," Act No. 300 (May 20, 1970), Title 1, Gazz. Uff. of May 27, 1970, No. 131. URL: http://www.minlavoro.it

71. Thüsing. Arbeitnehmerdatenschutz und Compliance (2010).

72. UK Privy Council, 6 April 1979, case Pau On v Lau Yiu Long. URL: http://www.e-lawresources.co.uk/Pao-on-v-Lau-Yiu-Long.php

73. Unclear Michael Kort. *Der Betrieb (DB).* 2011. P. 651, 653.

74. Universal Declaration of Human Rights of December 10, 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights

75. Абаев Ф. А. Правовое регулирование отношении по защите персональных данных работника в трудовом праве : автореф. дис. … канд. юрид. наук :12.00.05. Москва, 2014. 27 с.

76. 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.

77. Аномалії в цивільному праві України : навч.-практ. посіб. / відп. ред. Р. А. Майданик. Київ : Юстініан, 2007. 912 с.

78. Бем М. В., Городиський І. М. Стандарти захисту персональних даних в соціальній сфері. Львів: б.в., 2018. 110 с.

79. Бєлова Ю. Д. Цивільні правовідносини щодо персональних даних : дис. … д-ра філософії 081 «Право». Хмельницький, 2021. 248 с.

80. Бондаренко Э. Н., Иванов Д. В. Конфиденциальная информация в трудовых отношениях. Санкт-Петербург : Изд-во «Юрид. центр-Пресс». 2012. 152 с.

81. Брижко В. М., Радянська А. І., Швець М. Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ : Тріумф, 2006. 256 с.

82. Відповідальність за порушення у сфері захисту персональних даних. URL: https://ek.expertus.com.ua/recommendations/2616

83. Волосецький В. О. Іноземний досвід правового регулювання захисту персональних даних. *International Scientific Journal.* 2014. URL: https://www.inter-nauka.com/uploads/public/14815322304340.pdf

84. Гнатюк С. Л. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: аналітична доповідь. Київ, 2012. 51 с.

85. Гусов К. Н., Толкунова В. Н. Трудовое право : учебник. Москва : ТК Велби, Изд-во Проспект, 2003. 496 с.

86. Дворецкий А. В. Защита персональных данных работника по законодательству РФ: автореф. … дис. канд. юрид. наук: 12.00.05. Томск, 2005. 28 с.

87. Деякі питання практичного застосування Закону України «Про захист персональних даних» : Роз'яснення Міністерства юстиції України від 21.12.2011. URL : http://zakon0.rada.gov.ua/laws/show/n0076323-11

88. Дмитренко О. А. Право фізичної особина власні персональні дані в цивільному праві. України : автореф. дис. ... канд. юрид. наук : 12.00.03. Київ, 2010. 19 с.

89. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних : міжнародний документ від 08.11.2001. ULR: http://zakon3.rada.gov.ua/laws/show/994_363

90. Євробюлетень. URL: https://parlament.org.ua/wp-content/uploads/2016/10/eurobulet_12_2009_uk.pdf

91. Європейська комісія визначає стратегію посилення правил захисту даних ЄС від 04.11.2010 р. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_10_1462

92. Загальна декларація прав людини : міжнародний документ ООН від 10.12.1948. *Офіційний вісник України*. 2008. № 93. Ст. 3103.

93. Камінська Н. В. Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового регулювання. *Науковий вісник Національної академії внутрішніх справ*. 2015. № 3. С. 106–114.

94. Кардаш А. В. Інформація про особу та персональні дані: окремі аспекти співвідношення. *Форум права*. 2017. № 4. С. 87–92.

95. Кодекс законів про працю України : Закон від 10.12.1971 № 322-VIII. *Відомості Верховної Ради УРСР*. 1971. Дод. до № 50.

96. Кодекс України про адміністративні правопорушення : Закон від 07.12.1984 № 8073-X. *Відомості Верховної Ради УРСР*. 1984. № 51. Ст. 1122.

97. Комісія пропонує всебічну реформу захисту даних (25.01.2012). URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

98. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : міжнародний документ від 28.01.1981. URL: http://zakon5.rada.gov.ua/laws/show/994_326

99. Конвенція про захист прав людини і основоположних свобод (з протоколами): Конвенція Ради Європи від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

100. Кондратенко Н. М. Особливості розвитку правовідносин у сфері захисту персональних даних: історико-джерелознавчий аспект. *Форум права*. 2013. № 2. С. 241–247.

101. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

102. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України*. 2013. № 9-10. Ст. 88.

103. Куценко Р. В. Гарантії захисту прав працівників в Україні. *Трудове право*. 2018. № 1. С. 55–58.

104. Луценко О. Є. Правове регулювання проходження конкурсу на зайняття посад державної служби із застосуванням поліграфа. *Проблеми*

*законності*. 2019. Вип. 145. С. 140–151. doi: https://doi.org/10.21564/2414-990x.145.155428.

105. Михайлик А. С. Гарантії захисту персональних даних працівників в Україні: законодавче забезпечення. *Правові новели*. 2022. № 16. С. 29–34.

106. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. *Науковий вісник Ужгородського національного університету. Серія "Право"*. 2022. Вип. 72 (2). С. 82–87.

107. Михайлик А. С. Забезпечення захисту персональних даних працівників: невирішені питання. *Правове забезпечення соціальної безпеки в умовах євроінтеграційних процесів* : тези допов. учасн. ІІІ Міжн. наук.-практ. конф. (м. Київ, 26 листопада 2021 р.) / за ред. М. І. Іншина, М. Б. Мельник. Київ : ФОП Маслаков, 2021. С. 166–168.

108. Михайлик А. С. Сучасний стан та проблеми захисту персональних даних працівників в Україні в умовах цифрової трансформації. *Соціальне право*. 2021. № 4. С. 175–184.

109. Михайлик А. С. Щодо законодавчого забезпечення захисту персональних даних працівників в Україні відповідно до міжнародних стандартів. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття»* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали міжнар. наук.-практ. конф. (м. Одеса, 17 черв. 2022 р.) / за заг. ред. С. В. Ківалова. Одеса : Вид. дім «Гельветика», 2022. Т. 1. С. 598–601.

110. Михайлик А. С. Щодо захисту персональних даних працівників. *Правові виклики сучасності: захист прав людини в умовах пандемії* : матеріали ІІ міжнар. наук.-практ. онлайн конф. (м. Чернівці, 22 жовт. 2021 р.) [редкол.: Н.Д. Гетьманцева (голова), О.В. Кіріяк (відпов. секр.) та ін.]. Чернівці : Чернівец. нац. ун-т ім. Ю. Федьковича, 2021. С. 238–239.

111. Обуховська Т. І. Класифікація персональних даних та режиму доступу до них. *Вісник Національної академії державного управління.* 2013. № 1. С. 97–104.

112. ОДА зобов'язані надавати на запит інформацію про виплати чиновникам, – омбудсман. URL: https://radako.com.ua/news/oda-zobovyazani-nadavati-na-zapit-informaciyu-pro-viplati-chinovnikam-ombudsman

113. Оніщенко О. В. Захист персональних даних. *Юридичний вісник*. 2012. № 1 (22). С. 60–64.

114. Посібник з європейського права у сфері захисту персональних даних. Київ : К.І.С., 2020. 432 с.

115. Посібник з європейського права у сфері захисту персональних даних, 2018. https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf

116. Постанова Верховного Суду у складі колегії суддів Касаційного адміністративного суду від 16.04.2020 р., справа №804/4069/17. URL: https://zakononline.com.ua/court-decisions/show/88815240

117. Постанова Полтавського апеляційного суду у складі колегії суддів судової палати з розгляду цивільних справ від 01.07.2020 р., справа № 554/4546/19. URL: https://reyestr.court.gov.ua/Review/90614697

118. Технічні та організаційні засоби захисту персональних даних. URL: https://ek.expertus.com.ua/recommendations/2851

119. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 № 5076-VI. *Відомості Верховної Ради України.* 2013. № 27. Ст. 282.

120. Про Антимонопольний комітет України : Закон України від 26.11.1993 № 3659-XII. *Відомості Верховної Ради України.* 1993. № 50. Ст. 472.

121. Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III. *Офіційний вісник України*. 2001. № 1. Т. 1. Ст. 1.

122. Про визнання такими, що втратили чинність, деяких указів Президента України : Указ Президента України від 20.06.2019 № 419/2019. *Офіційний вісник України*. 2019. № 50. Ст. 1690.

123. Про внесення змін до деяких законодавчих актів України щодо обліку трудової діяльності працівника в електронній формі : Закон України від 05.02.2021 № 1217-IX. *Офіційний вісник України*. 2021. № 21. Ст. 882.

124. Про внесення змін до деяких законодавчих актів України : Закон України від 11.05.2004 № 1703-IV. *Офіційний вісник України.* 2004. № 22. Ст. 1483.

125. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. *Відомості Верховної Ради України.* 2011. № 32. Ст. 314.

126. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 № 361-IX. *Відомості Верховної Ради України*. 2020. № 25. Ст. 171.

127. Про запровадження обліку трудової діяльності працівника, фізичної особи-підприємця, фізичної особи, яка забезпечує себе роботою самостійно, в електронній формі : постанова Каб. Міністрів України від 27.11.2019 № 1084. *Офіційний вісник України*. 2020. № 3. Ст. 130.

128. Про затвердження документів у сфері захисту персональних даних : наказ Уповноваженого ВР з прав людини від 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

129. Про затвердження зразка бланка, технічного опису та Порядку оформлення, видачі, обміну, пересилання, вилучення, повернення державі, визнання недійсним та знищення паспорта громадянина України : постанова Каб. Міністрів України від 25.03.2015 № 302. *Офіційний вісник України*. 2015. № 40. Ст. 1188.

130. Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів : наказ М-ва юстиції України від 12.04.2012 № 578/5. *Офіційний вісник України.* 2012. № 34. Ст. 1272.

131. Про затвердження плану заходів щодо детінізації доходів та відносин у сфері зайнятості населення : розпорядження Каб. Міністрів України від 02.03.2010 № 359-р. *Урядовий кур'єр*. 24.03.2010. № 54.

132. Про затвердження Положення про військово-транспортний обов'язок : постанова Каб. Міністрів України від 28.12.2000 № 1921. *Офіційний вісник України*. 2008. № 50. Ст. 1665.

133. Про затвердження Положення про здійснення банками фінансового моніторингу : постанова Нац. банку України від 19.05.2020 № 65. *Офіційний вісник України*. 2020. № 60. Ст. 1920.

134. Про затвердження Порядку організації та ведення військового обліку призовників, військовозобов'язаних та резервістів : постанова Каб. Міністрів України ввід 30.12.2022 № 1487. URL: https://ek.expertus.com.ua/laws/16532

135. Про затвердження Типового регламенту місцевої державної адміністрації : постанова Каб. Міністрів України від 11.12.1999 № 2263. *Офіційний вісник України*. 1999. № 50. Ст. 2456.

136. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

137. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Офіційний вісник України*. 2010. № 49. Ст. 1604.

138. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР. *Відомості Верховної Ради України*. 1996. № 47. Ст. 256.

139. Про інформацію : Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

140. Про місцеві державні адміністрації : Закон України від 09.04.1999 № 586-XIV. *Відомості Верховної Ради України.* 1999. № 20. Ст. 190.

141. Про мобілізаційну підготовку та мобілізацію : Закон України від 21.10.1993 № 3543-XII. *Відомості Верховної Ради України*. 1993. № 44. Ст. 416.

142. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40-41. Ст. 1970.

143. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України.* 1992. № 22. Ст. 303.

144. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України.* 1992. № 22. Ст. 303.

145. Про оптимізацію системи центральних органів виконавчої влади : постанова Каб. Міністрів України від 10.09.2014 № 442. *Офіційний вісник України*. 2014. № 74. Ст. 2105.

146. Про Положення про Державну службу України з питань захисту персональних даних : Указ Президента України від 06.04.2011 № 390/2011. *Офіційний вісник України*. 2011. № 28. Ст. 1160.

147. Про практику розгляду судами трудових спорів : постанова Пленуму Верхов. Суду України від 06.11.1992 № 9. URL: http://zakon3.rada.gov.ua/laws/show/v0009700-92

148. Про проведення інвентаризації пенсійних справ : постанова Пенсійного фонду України від 03.09.2018 № 19-1. *Офіційний вісник України*. 2018. № 78. Ст. 2620.

149. Про прокуратуру : Закон України від 14.10.2014 № 1697-VII. *Відомості Верховної Ради України*. 2015. № 2-3. Ст. 12.

150. Рекомендації Комітету міністрів Ради Європи № R (87) 15 щодо використання персональних даних у сфері діяльності правоохоронних органів : міжнародний документ від 17.09.1987. URL: http://cyberpeace.org.ua/files/rekomendacia_km_radi_evropi_sodo_vikoristanna_personal_nih_danih__sektori_policii.pdf

151. Рекомендації Комітету міністрів Ради Європи № R (97) 5 щодо захисту медичних даних : міжнародний документ від 13.02.1997. URL: https://www.umj.com.ua/article/37381/rekomendacii-radi-yevropi-shhodo-zaxistumedichnix-danix

152. Рим О. Захист персональних даних працівників у Європейському Союзі. URL: https://www.researchgate.net/publication/344225298_Employee%27s_personal_data

_protection_in_European_Union_Zahist_personalnih_danih_pracivnikiv_u_Evropejskomu_Souzi-

153. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету*. 2013. Вип. 6-3 (1). С. 90–94.

154. Різак М. В. Правове регулювання відносин щодо персональних даних в Україні : монографія. Харків : Панов, 2016. 464 с.

155. Різак М. В. Створення реального правового механізму захисту персональних даних як необхідний елемент гарантування недоторканності приватного життя людини в умовах становлення інформаційного суспільства в Україні. *Науковий вісник Ужгородського національного університету. Серія: ПРАВО.* 2015. Вип. 35. Ч. ІІ. Т. 2. С. 190–193.

156. Рішення ЄСПЛ у справі «Барбулеску проти Румунії» (Bărbulescu v. Romania [GC]), № 61496/08 від 05.09.2017. URL: http://eurocourt.in.ua/Article.asp?AIdx=307

157. Рішення ЄСПЛ у справі «Копланд проти Сполученого Королівства» (Copland v. the United Kingdom), № 62617/00 від 03.04.2007. URL: https://international.vlex.com/vid/case-of-copland-v-870660049

158. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. *Офіційний вісник України.* 2012. № 9. Ст. 332.

159. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г. Устименка) від 30.10.1997 № 5-зп. *Офіційний вісник України*. 1997. № 46. Ст. 126.

160. Рішення Новозаводського районного суду міста Чернігова від 21.02.2020, справа №751/7922/19. URL: https://reyestr.court.gov.ua/Review/88045939

161. Робочий документ про загальне тлумачення статті 26(1) Директиви 95/46/ЕС від 24 жовтня 1995 р. РГ 114, Брюссель від 25.11.2005. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf

162. Висновок 2/2017 про обробку персональних даних на роботі. РГ 249, Брюссель від 08.06.2017. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf

163. Роз'яснення до Типового порядку обробки персональних даних Уповноважений ВР з прав людини від 08.01.2014. URL: https://zakon.rada.gov.ua/laws/show/n0001715-14#Text

164. Роз'яснення з питань здійснення ідентифікації клієнтів банків : Лист Національного банку України від 11.11.2011 № 48-104/2256-13461. URL: https://zakon.rada.gov.ua/laws/show/v1346500-11#Text

165. Романюк І. І. Законодавчі та теоретичні підходи до визначення поняття персональних даних та відмежування його від суміжних понять. *Актуальні питання публічного та приватного права*. 2014. № 1. С. 82–90.

166. Серебряник О. О. Інформація про особу як об’єкт цивільних прав : дис. ... канд. юрид. наук : 12.00.03. Івано-Франківськ, 2016. 209 с.

167. Сопілко І. М. Механизм захисту персональних даних: проблеми та перспективи. *Юридичний вісник*. 2013. № 2 (27). С. 66–70.

168. Сопілко І. М. Специфіка принципів окремих інститутів інформаційного права: порівняльно-правовий аналіз. *Юридичний вісник*. 2012. № 2 (23). С. 70–74.

169. Сопілко І. М. Щодо вдосконалення системи захисту персональних даних в процесі їх обробки. *Форум права.* 2013. № 1. С. 939–945.

170. Суд ЄС, C-342/12, «“Worten – Home Equipment SA” проти Контролюючого органу з дотримання умов праці» (Worten–Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)) від 30.05.2013. URL: https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf

171. Хартія Європейського Союзу про основні права. URL: https://ccl.org.ua/posts/2021/11/hartiya-osnovnyh-prav-yevropejskogo-soyuzu/

172. Хныкин Г. В. Особенности локального нормотворчества. *Практический журнал для руководителей и юристов «Законодательство».* 2005. № 4-5.

173. Цвірюк Д. В. Аналіз недоліків законодавства України у сфері захисту персональних даних. *Право і безпека*. 2013. № 4 (51). С. 58–64.

174. Чанишев Р. І. Поняття та класифікація персональних даних працівників. *Актуальні проблеми держави і права*. 2007. Вип. 30. С. 73–81

175. Чернобай А. М. Правові засоби захисту персональних даних працівннка : автореф. … дис. … канд.юрид. наук : 12.00.05. Одеса, 2006. 23 с.

176. Чернобай А.М. Правові засоби захисту персональних даних працівника : дис. ... канд. юрид. наук : 12.00.05. Одеса, 2006. 199 с.

177. Шишка Р. Б. До проблеми індивідуалізації фізичної особи. *Еволюція цивільного законодавства: проблеми теорії і практики :* матеріали міжнар. наук.-практ. конф. (м. Харків, 29-30 квіт. 2004 р.). Харків : Академія правових наук України, НДІ приватного права і підприємництва, НДІ інтелектуальної власності, Національна юридична академія ім. Я. Мудрого, 2004. С. 153–162.

178. Щербина А. О. Адміністративно-правове регулювання використання персональних даних суб'єктами владних повноважень в Україні : дис. … канд. юрид. наук : 12.00.07. Запоріжжя, 2020. 232 с.

179. Щодо персональний даних : Лист Державної служби України з питань захисту персональних даних від 02.04.2012 №10/1106-12. URL: https://dtkt.com.ua/show/2cid09507.html

180. Щодо порядку видачі в медичних закладах документів, що засвідчують тимчасову непрацездатність громадян : Лист Мін-ва охорони здоров`я від 12.06.2017 №3.04.02-Н-7698/6898-зв. URL: https://buhgalter911.com/uk/news/news-1032946.html

181. Яворська І., Микієвич М. Захист персональних даних у праві Європейського Союзу. *Вісник Львівського університету. Серія міжнародні відносини.* 2019. Вип. 46. С. 234–240.

182. Як запровадити захист персональних даних. URL: https://ek.expertus.com.ua/recommendations/3531

183. Як передавати персональні дані на запити третіх осіб. URL: https://ek.expertus.com.ua/recommendations/3536

# ДОДАТКИ

## ДОДАТОК А

## ПОЛОЖЕННЯ
## про порядок обробки та захисту персональних даних працівників та контрагентів

### 1. Загальні положення

1.1. Положення про порядок обробки та захисту персональних даних працівників та контрагентів (далі – Положення) визначає комплекс організаційних та технічних заходів для забезпечення захисту персональних даних працівників підприємства та контрагентів підприємства (фізичних осіб, які надають послуги підприємству, та фізичних осіб – отримувачів послуг підприємства, персональні дані яких обробляють під час реалізації договірних відносин; далі – контрагенти) від випадкових втрати або знищення, від незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних.

1.2. Положення розроблено на підставі Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI (далі – Закон № 2297) та Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14.

1.3. Положення є обов’язковим для виконання працівниками підприємства, які мають доступ до персональних даних та (або) обробляють персональні дані.

Працівників підприємства, які мають доступ до персональних даних та (або) обробляють персональні дані, ознайомлюють з цим Положенням під підпис. Копію Положення видають такому працівнику для використання у роботі.

1.4. Усі терміни у Положенні визначені відповідно до Закону № 2297, при цьому згідно із термінологією Закону № 2297 підприємство вважається володільцем персональних даних.

1.5. До персональних даних належать будь-які відомості чи сукупність відомостей про фізичну особу, за якими вона ідентифікується чи може бути конкретно ідентифікована.

1.6. Персональні дані працівників і контрагентів підприємства є об’єктами захисту. Підприємство прийняло на себе зобов’язання щодо захисту персональних даних працівників та контрагентів.

1.7. Персональні дані працівників та контрагентів підприємства обробляють на паперових носіях та за допомогою автоматизованої системи

(вкажіть назву автоматизованої системи (систем), наприклад, 1С, «Парус») (далі – Автоматизована система), а також інших програмних продуктів (Excel, Word тощо).

1.8. Під обробкою персональних даних розуміють будь-яку дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передавання), знеособлення, знищення персональних даних, зокрема з використанням інформаційних (автоматизованих) систем.

1.9. Персональні дані працівників обробляють у відділі кадрів та в бухгалтерії.

1.10. У відділі кадрів персональні дані працівників обробляють на паперових носіях (картотека особових карток (типова форма П-2), картотека військового обліку, особові справи, інші документи, що містять персональні дані працівників, зокрема трудові книжки, організаційно-розпорядчі документи, звітні та облікові форми) та в Автоматизованій системі.

1.11. У бухгалтерії персональні дані працівників обробляють на паперових носіях (організаційно-розпорядчі документи, бухгалтерські документи, звітні та облікові форми) та в Автоматизованій системі.

1.12. Персональні дані контрагентів обробляють у бухгалтерії та в інших підрозділах (вказати назви підрозділів, наприклад відділ збуту, відділ логістики, відділ кадрів, відділ договірної роботи тощо).

1.13. Персональні дані контрагентів обробляють на паперових носіях (договори, бухгалтерські документи, облікові форми тощо) та в Автоматизованій системі.

1.14. Для персональних даних працівників та контрагентів розпорядники відсутні. Працівники підприємства не вважаються розпорядниками персональних даних працівників та контрагентів.

1.15. Третіми особами у контексті Закону № 2297 є:

державні органи, яким персональні дані передають відповідно до законодавства (Пенсійний фонд, податкова інспекція, територіальні центри комплектування та соціальної підтримки, центри зайнятості, лікувально-профілактична установа, що проводить обов’язкові медичні огляди тощо);

будь-які особи, за винятком працівника або контрагента, підприємства як володільця персональних даних та Уповноваженого Верховної Ради України з прав людини, яким підприємство може передавати персональні дані.

1.16. Передання персональних даних третім особам та доступ третіх осіб до персональних даних відбуваються з урахуванням вимог Закону № 2297 у порядку, визначеному розділом 13 Положення.

1.17. Первинна профспілкова організація, що діє на підприємстві, самостійно забезпечує захист відомостей, наданих працівниками, які є членами

профспілки, і вважається володільцем таких персональних даних. Підприємство надає первинній профспілковій організації потрібну допомогу з питань захисту персональних даних. Порядок обробки та захисту персональних даних членів профспілки визначає відповідне положення, затверджене профспілковим комітетом.

1.18. В адміністративній будівлі ведуть відеофіксацію та (або) відеоспостереження з метою:

- запобігти неконтрольованому переміщенню матеріальних цінностей;
- попередити заподіяння шкоди здоров'ю працівників та відвідувачів підприємства.

У приміщеннях адміністративної будівлі, де ведуть відеофіксацію та (або) відеоспостереження, встановлюють попереджувальні знаки, які містять інформацію про володільця персональних даних та його контактні дані, за якими суб'єкт персональних даних може отримати інформацію, визначену частиною другою статті 12 Закону № 2297.

Матеріали відеофіксації та (або) відеоспостереження обробляє з дотриманням законодавства відповідальна за їх обробку особа, яку визначили наказом по підприємству.

Матеріали відеофіксації та (або) відеоспостереження зберігають на серверному обладнанні підприємства не довше 30 календарних днів. Доступ до матеріалів мають відповідальні працівники підприємства, для яких обов’язки обробляти такі матеріали містить посадова інструкція.

За необхідності строк зберігання таких матеріалів може бути продовжений за рішенням директора підприємства.

Доступ до матеріалів відеофіксації та (або) відеоспостереження мають директор підприємства, його перший заступник, працівники служби охорони, а також особа, визначена відповідальною за обробку матеріалів відеоспостереження, особа, відповідальна за організацію роботи із захисту персональних даних.

1.19. Працівник надає згоду щодо надання дозволу на обробку його персональних даних Пенсійним фондом України у разі, якщо роботодавець передає ПФУ сканкопії трудової книжки працівника та інших документів відповідно до постанови КМУ «Про запровадження обліку трудової діяльності працівника, фізичної особи — підприємця, фізичної особи, яка забезпечує себе роботою самостійно, в електронній формі» від 27.11.2019 № 1084.

## 2. Мета обробки персональних даних

2.1. Персональні дані працівників обробляють з метою реалізації трудових, соціально-трудових відносин, відносин у сфері управління персоналом, військового обліку військовозобов’язаних, призовників та

резервістів, охорони праці (відповідно до КЗпП, Законів України «Про професійні спілки, їх права та гарантії діяльності», «Про військовий обов'язок і військову службу», «Про охорону праці», колективного договору підприємства, статуту підприємства); відносин у сфері бухгалтерського і податкового обліку (відповідно до Податкового кодексу України, Законів України «Про бухгалтерський облік та фінансову звітність в Україні», «Про оплату праці»).

2.2. Обробка персональних даних працівників є необхідною для виконання передбаченого законом обов'язку підприємства як роботодавця, що використовує працю найманого персоналу, а саме для:

ведення кадрового діловодства;

підготовки визначеної законодавством статистичної та іншої звітності;

документаційного забезпечення, визначених у пункті 2.1 відносин, зокрема прав та обов'язків працівників і роботодавця у сфері праці.

2.3. Персональні дані контрагентів обробляють з метою реалізації договірних відносин під час здійснення підприємством господарської діяльності (відповідно до Господарського кодексу України, Цивільного кодексу України, згідно зі статутом підприємства), відносин у сфері бухгалтерського і податкового обліку (відповідно до Податкового кодексу України, Закону України «Про бухгалтерський облік та фінансову звітність в Україні», інших нормативно-правових актів у сфері бухгалтерського та податкового обліку).

## 2. Склад персональних даних працівників, що обробляють на підприємстві

3.1. Відповідно до визначеної мети обробки, нормативно-правових актів, специфіки діяльності підприємства, потреб управлінської діяльності, кваліфікаційних вимог до професій (посад) працівників, обробляють такі персональні дані працівників:

- прізвище, ім'я, по батькові;
- дата і місце народження;
- паспортні дані;
- номер ідентифікаційного коду (номер облікової картки платника податків);
- відомості з військового квитка , тимчасового посвідчення, приписного свідоцтва;
- відомості про трудову діяльність, що містить трудова книжка);
- відомості про освіту, наявність спеціальних знань або підготовки (за потреби, залежно від кваліфікаційних вимог до посади);
- відомості про наявність кваліфікаційної категорії (розряду, класу тощо);

- відомості про стан здоров’я (обробляють відповідно до статті 24 КЗпП в обсязі, необхідному для реалізації трудових відносин та для забезпечення вимог законодавства у сфері охорони праці);
- біографічні дані;
- відомості про ділові та особисті якості, зокрема, вказані у поданому при працевлаштуванні резюме (зокрема щодо рис характеру, особистих захоплень, звичок);
- відомості про родинний стан, членів родини в обсязі, необхідному для реалізації трудових відносин та забезпечення пільг і гарантій, передбачених трудовим законодавством;
- відомості про місце реєстрації та фактичне проживання, номери телефонів, адресу особистої електронної пошти;
- відомості про членство у професійних спілках;
- відомості, що підтверджують право на пільги та компенсації відповідно до законодавства (встановлення інвалідності, належність до категорії постраждалих від аварії на ЧАЕС, призначення пенсії, статус одинокої матері, опікуна, піклувальника, усиновлення дитини тощо);
- фотозображення.

3.2. На підприємстві не обробляють відомості про расове, національне або етнічне походження працівників, їх політичні, світоглядні переконання, членство в політичних партіях, відомості, що стосуються статевого життя.

3.3. Обробка персональних даних працівників про членство у професійних спілках, стан здоров’я (що згідно із законодавством належить до персональних даних, обробка яких становить особливий ризик для прав і свобод громадян) є необхідною для реалізації прав та виконання обов’язків володільця персональних даних у сфері трудових правовідносин відповідно до закону. Враховуючи цілі обробки, підприємство як володілець персональних даних не зобов'язане повідомляти Уповноваженого Верховної Ради з прав людини про обробку зазначених видів персональних даних (ст. 9 Закону № 2297, п. 1.2, 2.1.3 Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації, затвердженого наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14).

## 4. Склад персональних даних контрагентів, що обробляють на підприємстві

4.1. Відповідно до визначеної мети обробки, нормативно-правових актів, потреб господарської діяльності підприємство може обробляти такі персональні дані контрагентів:

- прізвище, ім’я, по батькові;
- відомості про місце реєстрації і місце фактичного проживання, номери телефонів, адреса електронної пошти;
- паспортні дані;
- номер ідентифікаційного коду (облікової картки платника податків).

4.2. Якщо надання послуг підприємству пов’язане з наявністю у фізичної особи – контрагента спеціальних знань та навичок, обробляють відомості про освіту, кваліфікацію на підставі наданих фізичною особою документів.

## 5. Обов’язки та права особи, відповідальної за організацію роботи, пов’язаної із захистом персональних даних на підприємстві

5.1. Для забезпечення реалізації норми частини першої статті 24 Закону № 2297, згідно з якою 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, директор підприємства призначає особу, відповідальну за організацію роботи, пов’язаної із захистом персональних даних на підприємстві (за її згодою) (далі — Відповідальна особа). Наказ доводять до відома Відповідальної особи під підпис.

5.2. Відповідальна особа:

5.2.1. Інформує та консультує керівництво та працівників підприємства з питань додержання законодавства про захист персональних даних.

5.2.2. Взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його Секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

5.2.3. Забезпечує реалізацію прав суб’єктів персональних даних.

5.2.4. У разі виявлення порушень законодавства про захист персональних даних та (або) цього Положення повідомляє про це директора підприємства щоби вжити необхідні заходи.

5.2.5. Аналізує загрози безпеці персональних даних.

5.2.6. Відстежує зміни у законодавстві про захист персональних даних, за необхідності ініціює внесення змін чи доповнень до цього Положення.

5.2.7. Погоджує проєкти положень про структурні підрозділи, працівники яких обробляють персональні дані, та посадових інструкцій працівників, які обробляють персональні дані або мають доступ до них, за необхідності ініціює внесення необхідних змін та доповнень до положень про структурні підрозділи та посадових інструкцій.

5.2.8. Фіксує факти порушень режиму захисту персональних даних у порядку, визначеному розділом 12 Положення.

5.3. Відповідальна особа має право:

5.3.1. На доступ до будь-яких персональних даних, які обробляють на підприємстві, та до всіх приміщень підприємства, де оброблюють такі дані.

5.3.2. Перевіряти, як працівники підприємства дотримуються законодавства у сфері захисту персональних даних та виконують вимоги Положення.

5.3.3. Брати участь у службових розслідуваннях з питань порушень порядку обробки та захисту персональних даних.

5.3.4. Вносити директору підприємства пропозиції про розмежування режиму доступу працівників до обробки персональних даних відповідно до їх посадових обов'язків.

## 6. Права та обов'язки працівників та контрагентів як суб'єктів персональних даних

6.1. Відповідно до Закону № 2297 працівник як фізична особа, персональні дані якої обробляє підприємство:

6.1.1. Є суб'єктом персональних даних.

6.1.2. Має право:

- знати про місцезнаходження своїх персональних даних, мету їх обробки;
- на доступ до своїх персональних даних;
- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передають його персональні дані;
- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням;
- на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
- звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради з прав людини або до суду;
- вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди на обробку персональних даних (наприклад, у разі відмови працівника від передання його персональних даних банківській установі в межах реалізації зарплатного карткового проєкту та за бажання отримувати заробітну плату особисто в бухгалтерії);
- знати механізм автоматичної обробки персональних даних;
- інші права, визначені статтею 8 Закону № 2297.

Інформацію про права у сфері захисту персональних даних, володільця персональних даних, третіх осіб, яким можуть передавати персональні дані, доводять до працівника під час прийняття на роботу одночасно зі збором

персональних даних, необхідних для реалізації трудових відносин, відповідно до статті 12 Закону № 2297, у порядку, визначеному розділом 8 «Збирання та оновлення персональних даних працівників» Положення.

6.1.3. Зобов'язаний повідомляти підприємство про зміну своїх персональних даних, що підлягають обробці, у порядку, визначеному у пункті 8.7 Положення.

6.2. Контрагент як суб'єкт персональних даних має права у сфері захисту персональних даних згідно зі статтею 8 Закону № 2297, зокрема, має право 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, право застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних; право звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради з прав людини або до суду.

До укладення цивільно-правового договору з підприємством у контрагента як суб'єкта персональних даних повинна бути можливість отримати весь комплекс відомостей, визначених статтею 12 Закону № 2297, а саме:

- про володільця персональних даних;
- склад і зміст зібраних персональних даних;
- права у сфері захисту персональних даних;
- мету збору персональних даних;
- третіх осіб, яким передають персональні дані володільця.

## 7. Обов'язки працівників підприємства, які обробляють персональні дані

Працівники підприємства, які обробляють персональні дані:

7.1. Мають бути обізнані з вимогами Закону № 2297 та інших нормативно-правових актів у сфері захисту персональних даних.

7.2. Зобов'язані:

7.2.1. Використовувати персональні дані лише відповідно до професійних чи службових або трудових обов'язків, запобігати втраті персональних даних або їх неправомірному використанню;

7.2.2. Не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків (крім випадків, передбачених законом), при цьому таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом;

7.2.3. Терміново повідомляти Відповідальну особу в разі:

втрати або неумисного знищення носіїв інформації з персональними даними;

втрати ними ключів від приміщень, сейфів, шаф, де зберігаються персональні дані;

якщо ідентифікаційні дані для входу в Автоматизовану систему стали відомі іншим особам, за винятком системного адміністратора підприємства;

виявлення спроби несанкціонованого доступу до персональних даних.

7.2.4. При звільненні з роботи або переведенні на іншу посаду своєчасно передати керівнику структурного підрозділу або іншому працівнику, визначеному керівництвом підприємства, носії інформації, що містять персональні дані, які були отримані або створені особисто чи спільно з іншими працівниками під час виконання посадових обов'язків.

## 8. Збирання та оновлення персональних даних працівників

8.1. Збирання персональних даних працівників є складовою процесу обробки таких персональних даних, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

8.2. Обробку (зокрема збирання) персональних даних, зазначених у пункті 3.1 Положення, провадять на підставі пункту 5 частини першої статті 11 Закону № 2297 – для виконання передбаченого законом обов'язку підприємства як роботодавця, що використовує працю найманих працівників.

8.3. Відповідно до частини другої статті 12 Закону № 2297 суб'єкта персональних даних мають повідомити про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені Законом № 2297, мету збору персональних даних та осіб, яким передаються його персональні дані, – у момент збору персональних даних, якщо персональні дані збирають у суб'єкта персональних даних.

Із метою забезпечення наведеної норми Закону № 2297 працівник відділу кадрів підприємства, який оформлює прийняття на роботу:

- роз'яснює претенденту на посаду підстави для обробки його персональних даних відповідно до Закону № 2297.
- повідомляє про те, що володільцем персональних даних, які збирають, є підприємство, роз'яснює, які персональні дані оброблятимуть та з якою метою, інформує про третіх осіб, яким передаватимуть або можуть передавати персональні дані після укладення трудового договору (органи Пенсійного фонду, податкової служби, територіальні центри комплектування та соціальної підтримки, фонди соціального страхування тощо).
- повідомляє претендента на посаду про його права як суб'єкта персональних даних, визначені статтею 8 Закону № 2297, у спосіб ознайомлення претендента з витягом із Закону № 2297 (див.

Додаток 1), за потреби надає необхідні пояснення щодо реалізації зазначених прав.

- інформує претендента на посаду, що підприємство вживає всіх необхідних заходів щодо захисту персональних даних своїх працівників, а безпосередню обробку персональних даних провадитимуть працівники, які надали письмові зобов'язання про нерозголошення персональних даних, які стали відомі під час виконання службових обов'язків.

8.4. Відмітку про повідомлення оформлюють на зворотному боці аркуша наказу про прийняття на роботу таким чином:

Повідомлений про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені Законом України «Про захист персональних даних», мету збору персональних даних та осіб, яким передають або можуть передавати мої персональні дані.

Підпис працівника Ініціали,
Дата прізвище
працівника

8.5. Ураховуючи, що згідно з частиною першою статті 6 Закону № 2297, обробка персональних даних має здійснюватися відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки, інформація про підприємство як володільця персональних даних працівників, склад та зміст персональних даних працівників, що обробляють, мету такої обробки, третіх осіб, яким передають або можуть передавати персональні дані, права працівників у сфері захисту персональних даних (в актуальному стані) (див. Додаток 1), розміщують на інформаційних стендах у відділі кадрів, у вестибюлі підприємства та на внутрішньому (Інтранет) сайті підприємства.

8.6. При укладанні трудового договору персональні дані вносять до Автоматизованої системи та картотеки персональних даних.

8.7. Аналогічний пункт можна додати до трафаретної форми на обробку персональних даних, яку заповнює працівник при прийнятті на роботу.

8.8. Персональні дані мають бути точними, достовірними та оновлюватися за потреби, визначеної метою їх обробки. Про зміну персональних даних, що підлягають обробці, працівники підприємства повідомляють відділ кадрів у п'ятиденний строк із наданням відповідних документів або їхніх копій.

8.8. У разі виявлення факту обробки відомостей про працівника, які не відповідають дійсності, такі відомості мають бути виправлені або знищені.

8.9. Контроль за питаннями, пов'язаними з повідомленням працівників про володільця персональних даних, склад та зміст даних, що збирають, мету обробки даних, права у сфері захисту персональних даних, покладають на начальника відділу кадрів.

## 9. Збирання персональних даних контрагентів

9.1. Збирання персональних даних контрагентів є складовою процесу обробки таких персональних даних, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

9.2. Підставою для обробки персональних даних контрагентів є укладення та виконання правочину, стороною якого є 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 (п. 3 ч. 1 ст. 11 Закону № 2297).

9.3. Питання, пов'язані з обробкою персональних даних контрагентів, зокрема повідомлення про володільця персональних даних, склад та зміст зібраних персональних даних, права контрагента як суб'єкта персональних даних, визначені Законом № 2297, мету збору персональних даних та осіб, яким передають персональні дані, порядок використання персональних даних контрагента працівниками підприємства, врегульовують у цивільно-правовому договорі, що укладають з контрагентом (договір про надання послуг тощо).

9.4. Факт повідомлення про права у сфері захисту персональних даних, володільця персональних даних, склад та зміст, мету збору персональних даних, третіх осіб, яким можуть передавати персональні дані, підтверджує підпис контрагента в договорі.

9.5. При укладанні договору персональні дані контрагента вносять до Автоматизованої системи. Примірник договору долучають до відповідної справи з договорами.

9.6. У разі виявлення факту обробки відомостей про контрагента, які не відповідають дійсності, такі відомості мають бути виправлені або знищені.

9.7. У разі зміни визначеної у пункті 2.3 мети обробки персональних даних контрагентом має бути надана згода на обробку його даних відповідно до зміненої мети, якщо нова мета обробки є несумісною з попередньою.

9.8. Контроль за питаннями, пов'язаними із дотриманням законодавства у сфері захисту персональних даних під час збирання персональних даних контрагентів, покладають на керівників структурних підрозділів, в яких оформлюють відповідні цивільно-правові договори.

## 10. Зберігання та знищення персональних даних працівників та контрагентів

10.1. Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.

10.2. Персональні дані працівників та контрагентів обробляють у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, та зберігають

не довше, ніж це необхідно відповідно до їх законного призначення та мети їх обробки, якщо інше не передбачено законодавством у сфері архівної справи та діловодства.

Так, документи, що містять персональні дані працівників та контрагентів (особові картки, особові справи, накази з кадрових питань, цивільно-правові договори тощо), зберігають упродовж строків, визначених Переліком типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів, затвердженим наказом Мін'юсту від 12.04.2012 № 578/5 (особові справи, особові картки, накази з кадрових питань тривалого строку зберігання – 75 років).

10.3. Персональні дані працівників та контрагентів видаляють або знищують в порядку, встановленому відповідно до вимог закону. Відбір для знищення документів з персональними даними, терміни зберігання яких закінчилися, провадить експертна комісія підприємства, склад якої визначає наказом директор підприємства.

10.4. Персональні дані, зібрані з порушенням вимог Закону № 2297, підлягають знищенню у встановленому законодавством порядку.

10.5. Персональні дані знищують у спосіб, що виключає подальшу можливість поновити такі персональні дані.

**11. Використання персональних даних працівниками підприємства**

11.1. Під використанням персональних даних згідно зі статтею 10 Закону № 2297 розуміються будь-які дії підприємства як володільця персональних даних працівників та контрагентів щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробляти персональні дані іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюють за згодою суб'єкта персональних даних чи відповідно до закону.

11.2. Доступ до персональних даних працівників мають працівники бухгалтерії та відділу кадрів, а також директор підприємства, його заступники, юрисконсульт, адміністратор системи відповідно до посадових обов'язків обсягом, необхідним для виконання таких обов'язків.

11.3. Доступ до персональних даних контрагентів мають працівники бухгалтерії, інших відділів, функції яких передбачають необхідність обробляти персональні дані (вказати назви відділів, наприклад, відділ збуту, відділ логістики, відділ кадрів), а також директор підприємства, його заступники, юрисконсульт, адміністратор системи відповідно до посадових обов'язків обсягом, необхідним для виконання таких обов'язків.

11.4. Працівники підприємства, які працюють з персональними даними, а також члени комісії (уповноважений) із соціального страхування підприємства та експертної комісії підприємства, дають письмове зобов'язання про

нерозголошення персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням посадових чи службових обов'язків, за формою, наведеною у Додатку 2.

11.5. Право на доступ до персональних даних та їх обробку надають працівникам підприємства лише після надання зобов'язання про нерозголошення персональних даних.

11.6. На працівників відділу кадрів, у посадових інструкціях яких передбачено відповідну функцію, покладено обов'язок щодо отримання зобов'язань.

11.7. Зобов'язання про нерозголошення персональних даних реєструють у Журналі реєстрації зобов'язань про нерозголошення персональних даних (форму Журналу наведено у Додатку 3). Нумерація у Журналі ведуть наростаючим підсумком, починаючи з № 1.

11.8. За Журналом реєстрації зобов'язань про нерозголошення персональних даних працівників ведуть облік фактів надання та позбавлення працівників права доступу до персональних даних та їх обробки.

11.9. Датою надання права доступу до персональних даних та їх обробки вважається дата надання зобов'язання.

11.10. Датою позбавлення права доступу до персональних даних та їх обробки вважається дата звільнення працівника або дата переведення на посаду, виконання обов'язків за якою не пов'язано з обробкою персональних даних.

11.11. Після реєстрації зобов'язання формують в окрему справу «Зобов'язання працівників підприємства щодо нерозголошення персональних даних». Цю справу та Журнал реєстрації зобов'язань про нерозголошення персональних даних включають до номенклатури справ відділу кадрів.

11.12. Відповідальним за забезпечення збереженості справи та Журналу, зазначених у пункті 11.11 Положення, є начальник відділу кадрів.

11.13. Працівники підприємства, які працюють з персональними даними, проходять регулярне навчання з питань захисту персональних даних, яке проводить не рідше одного разу на рік юрисконсульт підприємства (або Відповідальна особа; або іншою посадова особа, вказати, ким саме).

11.14. Працівникам підприємства, які працюють з персональними даними, заборонено залишати документи з персональними даними на робочих столах без нагляду.

## 12. Облік порушень режиму захисту персональних даних

12.1. Про факти порушень режиму захисту персональних даних керівники структурних підрозділів підприємства негайно повідомляють Відповідальну особу.

12.2. Факти порушень режиму захисту персональних даних фіксують в актах, що складає Відповідальна особа.

12.3. За необхідності за фактами порушень режиму захисту персональних даних директор підприємства призначає службове розслідування.

12.4. За результатами службового розслідування на працівників, винних у порушеннях, можуть бути накладені дисциплінарні стягнення.

## 13. Передання персональних даних третім особам та надання третім особам до персональних даних

13.1. Поширення персональних даних передбачає дії щодо передавання відомостей про працівника (контрагента) за його згодою.

13.2. Поширення персональних даних без згоди працівника (контрагента) або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

13.3. Сторона, якій передають персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог Закону № 2297.

13.4. Для реалізації карткового зарплатного проєкту працівник укладає відповідний договір з банківською установою. Підприємство як володілець персональних даних не передає персональні дані працівників банківській установі.

13.5. Порядок доступу третіх осіб до персональних даних працівників (контрагентів) визначають відповідно до вимог закону.

13.6. Суб’єкт відносин, пов’язаних з персональними даними, подає запит щодо доступу (далі – запит) до персональних даних підприємству як володільцю персональних даних.

У запиті мають бути зазначені:

13.6.1. Прізвище, ім’я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника).

13.6.2. 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).

13.6.3. Прізвище, ім’я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, щодо якої зробили запит.

13.6.4. Відомості про базу персональних даних, стосовно якої подають запит, чи відомості про володільця чи розпорядника персональних даних.

13.6.5. Перелік персональних даних, що запитують.

13.6.6. Мета та (або) правові підстави для запиту.

13.7. У разі отримання запиту від третіх осіб на доступ до персональних даних працівника (контрагента) такий доступ надають за його згодою або згідно зі статтею 16 Закону № 2297.

13.8. Юрисконсульт разом із Відповідальною особою вивчають запит на предмет його задоволення (зокрема щодо наявності відомостей, вказаних у п. 13.6 Положення) упродовж 10 робочих днів із дня надходження запиту (відповідно до ч. 5 ст. 16 Закону № 2297).

Упродовж цього строку підприємство має довести до відома особи, яка подала запит, що його буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Запит задовольняють протягом 30 календарних днів із дня його надходження, якщо інше не передбачено законом.

13.9. Доступ до персональних даних третій особі не надають, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону № 2297 або неспроможна їх забезпечити. Підтвердження зобов'язання щодо забезпечення виконання вимог Закону оформлюють у вигляді розписки.

13.10. Заборонено повідомляти персональні дані третім особам (зокрема банкам, кредитним спілкам, колекторським організаціям, посольствам, консульствам тощо) телефоном або електронною поштою.

Якщо працівнику відомо, що певна установа (банк, кредитна спілка, посольство тощо) може звертатися на підприємство з метою отримання чи підтвердження інформації, що належить до персональних даних, працівнику рекомендовано звернутися заздалегідь до відділу кадрів (бухгалтерії) підприємства з проханням видати довідку, яка містить інформацію, яку можуть запитувати, для надання її за потреби установі-запитувачу.

13.11. Працівник (контрагент) має право одержувати будь-які відомості про себе, що обробляє підприємство, без зазначення мети запиту.

## 14. Захист персональних даних при їх обробці

14.1. Захист персональних даних в Автоматизованій системі.

14.1.1. Право доступу до Автоматизованої системи надають працівникам підприємства, в посадових інструкціях яких передбачено функції з обробки даних в Автоматизованій системі та які надали письмове зобов'язання щодо нерозголошення персональних даних.

14.1.2. Працівників підприємства допускають до обробки персональних даних в Автоматизованій системі лише після їх ідентифікації (логін, пароль).

14.1.3. Доступ осіб, які не пройшли процедуру ідентифікації, блокують.

14.1.4. Автоматизовану систему в обов'язковому порядку забезпечують антивірусним захистом та засобами безперебійного живлення елементів системи. Відповідні заходи забезпечує адміністратор системи.

14.1.5. При переведенні на іншу посаду, що не передбачає обробки персональних даних, або звільненні працівника, який мав право на обробку персональних даних в Автоматизованій системі, працівник відділу кадрів, що оформлює переведення (звільнення) повідомляє про це електронною поштою адміністратора системи, який припиняє (закриває) доступ працівника до Автоматизованої системи.

14.2. Захист персональних даних у формі картотеки.

14.2.1. Начальники структурних підрозділів, в яких обробляють персональні дані, забезпечують захист персональних даних на паперових носіях від несанкціонованого доступу.

14.2.2. До роботи з персональними даними на паперових носіях допускають лише працівників, у посадових інструкціях яких передбачено відповідні функції та які надали письмове зобов'язання щодо нерозголошення персональних даних.

14.2.3. Двері у приміщення, де зберігають паперові носії, що містять персональні дані, обладнують замками.

14.2.4. Паперові носії з персональними даними зберігають у шафах і сейфах, що надійно зачиняються (з урахуванням вимог нормативно-правових актів, що регламентують ведення відповідних картотек).

14.2.5. У приміщенні відділу кадрів зона для відвідувачів і зону для роботи працівників відділу з документами розмежовують (вказати спосіб розмежування зон, приміром за допомогою стійки тощо).

## 15. Облік операцій, пов'язаних з обробкою персональних даних та доступом до них, на підприємстві

15.1. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) на підприємстві обробляють у спосіб, що унеможливлює несанкціонований доступ до них сторонніх осіб.

Із цією метою обліковують операції, пов'язані з обробкою персональних даних та доступом до них, під час чого зберігається інформація про:

- дату, час та джерело збирання персональних даних;
- зміну персональних даних;
- перегляд персональних даних;
- передавання (копіювання) персональних даних;

- дату та час видалення або знищення персональних даних;
- працівника, який здійснив одну із указаних операцій;
- мету та підстави зміни, перегляду, передавання та видалення або знищення персональних даних.

15.2. У випадках, коли обробку персональних даних здійснюють за допомогою Автоматизованої системи, вказана інформація фіксується автоматично.

15.3. Обліковують операції, пов’язані з обробкою персональних даних на паперових носіях, у Журналі обліку операцій, пов’язаних з обробкою персональних даних (див. Додаток 4). Такий Журнал веде кожен підрозділ підприємства, в якому обробляють такі дані, окремо щодо персональних даних контрагентів та працівників.

15.4. Інформацію про облік операцій, пов’язаних з обробкою персональних даних та доступом до них, зберігають упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції.

| | | |
|---|---|---|
| Особа, відповідальна за організацію роботи із захисту персональних даних | Підпис | Ініціали, прізвище |

Візи (рекомендовано погодження Положення посадовими особами, які брали участь у його розробці, наприклад головний бухгалтер, начальник відділу кадрів, юрисконсульт, адміністратор системи)

**Додаток 1**
до Положення про порядок обробки
та захисту персональних даних
працівників та контрагентів

_____
(назва підприємства)

## ІНФОРМАЦІЯ
## про обробку персональних даних працівників

Шановні колеги!

З повагою до своїх працівників та букви закону підприємство прагне забезпечувати всі ваші права та гарантії, у т. ч. щодо захисту ваших персональних даних.

Відповідно до Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI (далі –Закон № 2297) та інших актів законодавства України, такі відомості про людину, як її національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальне становище, адреса, дата і місце народження, місце проживання тощо належать до **персональних даних** і є об'єктами захисту.

У термінології Закону № 2297 підприємство вважається **володільцем персональних даних.**

Для виконання своїх обов'язків у сфері трудових відносин підприємство як роботодавець обробляє персональні дані працівників відповідно до закону (п. 5 ч. 1 ст. 11 Закону № 2297).

Під обробкою персональних даних розуміють будь-яку дію або сукупність дій, таких як збирання, реєстрація, зберігання, знищення персональних даних тощо, зокрема з використанням інформаційних (автоматизованих) систем (ст. 2 Закону № 2297).

**Мета обробки, склад і зміст персональних даних працівників**

Мета обробки підприємством персональних даних працівників — реалізація трудових, соціально-трудових відносин, відносин у сфері управління персоналом, військового обліку, охорони праці (відповідно до КЗпП, Законів України «Про охорону праці», «Про професійні спілки, їх права та гарантії діяльності», «Про військовий обов'язок і військову службу», колективного договору підприємства, статуту підприємства); відносин у сфері бухгалтерського і податкового обліку (відповідно до Податкового кодексу України, Законів України «Про бухгалтерський облік та фінансову звітність в Україні», «Про оплату праці»).

Приміром, відомості про наявність у працівників двох дітей віком до 15 років обробляють для надання додаткової відпустки, а відомості про встановлення інвалідності – для створення належних умов праці, які підходять працівнику за станом здоров'я, та надання щорічної відпустки збільшеної тривалості.

Відповідно до визначеної мети обробки, нормативно-правових актів, специфіки діяльності підприємства, потреб управлінської діяльності, кваліфікаційних вимог до професій (посад) працівників, обробляють такі персональні дані працівників: прізвище, ім'я, по батькові, дата і місце народження, паспортні дані, номер ідентифікаційного коду (номер облікової картки платника податків), відомості з військового квитка (тимчасового посвідчення, приписного свідоцтва), відомості про трудову діяльність, що містяться у трудовій книжці, відомості про освіту, наявність спеціальних знань або підготовки (за потреби, залежно від кваліфікаційних вимог до посади); відомості про наявність кваліфікаційної категорії (розряду, класу тощо); відомості про стан здоров'я (обробляють відповідно до ст. 24 КЗпП в обсязі, необхідному для реалізації трудових відносин та для забезпечення вимог законодавства у сфері охорони праці); біографічні дані; відомості про ділові та особисті якості, зокрема, вказані у поданому при працевлаштуванні резюме (зокрема щодо рис характеру, особистих захоплень, звичок); відомості про родинний стан, членів родини в обсязі, необхідному для реалізації трудових відносин; відомості про фактичне місце проживання, номери телефонів, адресу особистої електронної пошти; відомості про членство у професійних спілках; відомості, що підтверджують право на пільги та компенсації відповідно до законодавства; фотозображення.

**Обробка і захист персональних даних працівників**

Наше підприємство вживає необхідних технічних і організаційних заходів щодо захисту персональних даних працівників.

Персональні дані працівників обробляють виключно працівники підприємства, які надали письмові зобов'язання про нерозголошення персональних даних інших осіб, що стали відомі у зв'язку з виконанням посадових обов'язків.

Персональні дані працівників передають в необхідних обсягах та відповідно до законодавства органам Пенсійного фонду, податкової служби, територіальним центрам комплектування та соціальної підтримки, іншим органам державної влади чи місцевого самоврядування для виконання ними своїх повноважень, передбачених законом.

У разі отримання запиту від третіх осіб на доступ до персональних даних працівника такий доступ надають за його згодою або згідно зі статтею 16 Закону № 2297.

Строки зберігання персональних даних, визначають згідно зі строками зберігання відповідних документів, встановленими законодавством України з метою захисту соціальних та трудових прав громадян, після чого персональні дані видаляють або знищують у визначеному законодавством порядку.

**Права суб'єкта персональних даних у сфері захисту персональних даних**

Відповідно до статті 8 Закону № 2297:

1. Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

2. Суб'єкт персональних даних має право:

1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передають його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за 30 календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляють його персональні дані, а також отримувати зміст таких персональних даних;

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

6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляють незаконно чи вони є недостовірні;

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

8) звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради з прав людини або до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

11) відкликати згоду на обробку персональних даних;

12) знати механізм автоматичної обробки персональних даних;

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

З повагою,
адміністрація підприємства

Додаток 2
до Положення про порядок
обробки та захисту персональних
даних працівників та контрагентів

_____ (назва підприємства)

_____ (назва посади керівника підприємства)

_____ (прізвище, ім'я, по батькові керівника)

_____ (назва посади працівника)

_____ (прізвище, ім'я, по батькові працівника)

**ЗОБОВ'ЯЗАННЯ**
**про нерозголошення**
**персональних даних**

_____ № _____
(дата)

_____
(місце складання документа)

Відповідно до статті 10 Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI зобов'язуюсь не розголошувати в будь-який спосіб персональні дані, які мені довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом.

Це зобов'язання залишається чинним після припинення моєї діяльності, пов'язаної з обробкою персональних даних у *(назва підприємства),* крім випадків, установлених законом.

Мене поінформовано про відповідальність за порушення законодавства про захист персональних даних.

_____
(підпис)

Додаток 3
до Положення про порядок обробки
та захисту персональних даних
працівників та контрагентів

**ЖУРНАЛ**
**реєстрації зобов'язань про нерозголошення персональних даних**

| **з/п** | **Прізвище, ім'я, по батькові** | **Посада** | **Дата надання зобов'язання** | **Дата позбавлення права доступу до персональних даних та їх обробки** | **Причина позбавлення права доступу до персональних даних та їх обробки (звільнення, переведення на посаду, обов'язки за якою не пов'язані з обробкою персональних даних)** |
|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Додаток 4
до Положення про порядок обробки
та захисту персональних даних
працівників та контрагентів

**ЖУРНАЛ**

**обліку операцій, пов’язаних з обробкою персональних даних**

| **з/п** | **Прізвище, ім’я, по батькові працівника, яким проведена операція з персональними даними** | **Посада** | **Дата та час операції з персональними даними** | **Категорія операції з персональними даними** | **Опис операції з персональними даними (із зазначенням джерела отримання персональних даних для категорії 1 і мети та підстави для категорій 2–5)** |
|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Категорії операцій з персональними даними:**

1 – Первинне збирання персональних даних;
2 – Зміна персональних даних;
3 – Перегляд персональних даних;
4 – Передача (копіювання) персональних даних;
5 – Видалення або знищення персональних даних.

# ДОДАТОК Б

## СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

*Наукові праці, в яких відображені основні результати дослідження:*

1. Михайлик А. С. Сучасний стан та проблеми захисту персональних даних працівників в Україні в умовах цифрової трансформації. *Соціальне право*. 2021. № 4. С. 200–207.
2. Михайлик А. С. Гарантії захисту персональних даних працівників в Україні: законодавче забезпечення. *Правові новели*. 2022. № 16. С. 29–34.
3. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. *Науковий вісник Ужгородського національного університету. Серія "Право"*. 2022. Вип. 72 (2). С. 82–87.
4. Mykhailyk A. S. International legal standards in the field of protection of personal data of employees. *The scientific heritage*. 2022. № 95(95). P. 35–38.

*Наукові праці, в яких засвідчено апробацію матеріалів дослідження:*

1. Михайлик А. С. Щодо захисту персональних даних працівників. *Правові виклики сучасності: захист прав людини в умовах пандемії* : матеріали II міжнар. наук.-практ. онлайн конф. (м. Чернівці, 22 жовт. 2021 р.) / [редкол.: Н. Д. Гетьманцева (гол.), О. В. Кіріяк (відп. секр.) та ін.]. Чернівці : Чернівец. нац. ун-т ім. Ю. Федьковича, 2021. С. 238–239.
2. Михайлик А. С. Забезпечення захисту персональних даних працівників: невирішені питання. *Правове забезпечення соціальної безпеки в умовах євроінтеграційних процесів* : тези допов. учасн. III міжнар. наук.-практ. конф. (м. Київ, 26 листоп. 2021 р.) / за ред. М. І. Іншина, М. Б. Мельник. Київ : ФОП Маслаков, 2021. С. 166–168.
3. Михайлик А. С. Щодо законодавчого забезпечення захисту персональних даних працівників в Україні відповідно до міжнародних стандартів. *Європейський вибір України, розвиток науки та національна*

*безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття»* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали міжнар. наук.-практ. конф. (м. Одеса, 17 черв. 2022 р.) / за заг. ред. С. В. Ківалова. Одеса : Вид. дім «Гельветика», 2022. Т. 1. С. 598–601.