

УДК 349.2; 341.1

DOI <https://doi.org/10.32837/apdp.v0i85.1872>

О. М. Рим

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

Постановка проблеми. Сьогодні забезпечення розумного рівня захисту персональних даних особи в контексті зайнятості постало перед новими викликами, котрі диктує науково-технічний прогрес. Більшість людей значну частину свого часу проводять на роботі. Водночас вони оточені різноманітними пристроями та засобами, які в той чи інший спосіб можуть фіксувати їхні дії чи бездіяльність. З огляду на це цифрові технології, що пропонують нові можливості для покращення продуктивності трудових процесів та дистанційної праці, можуть одночасно призвести до розмивання меж між робочим та приватним життям, створюючи значні проблеми для приватного життя працівника.

Наведене потребує міцної та узгодженої системи захисту й така в Європейському Союзі запроваджена Регламентом (ЄС) 2016/679 від 27 квітня 2016 року «Про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних» [1]. Автори цього Регламенту поставили перед собою грандіозне завдання: скоординувати двадцять вісім держав-членів, діяльність їхніх відповідних органів захисту даних, національне законодавство та судову практику, що аж ніяк не є легким завданням. Такі підвищені очікування базувались на обіцянках Європейської Комісії створити «сильну, чітку та єдину законодавчу базу на європейському рівні» з питань обробки даних, яка б ліквідувала розбіжності національного правового регулювання [2, с. 182].

Аналіз останніх досліджень і публікацій. Питання правового регулювання обробки персональних даних у Європейському Союзі вивчало багато науковців. Різноманітні аспекти захисту прав та інтересів ідентифікованих осіб у ЄС були предметом дослідження таких учених, як М. Микієвич, О. Шевчук, І. Яворська та багатьох інших. Проте певні аспекти цієї проблеми залишаються поза увагою науковців і потребують детального вивчення. А саме необхідно комплексно проаналізувати особливості обробки персональних даних у сфері працевлаштування, адже євроінтеграційні прагнення України вимагають погодження вітчизняного законодавства з європейськими стандартами.

Метою статті є вивчення процедури обробки персональних даних працівників у Європейському Союзі.

Виклад основного матеріалу дослідження. Положення Регламенту (ЄС) 2016/679 наділяють працівників такими можливостями:

- правом бути поінформованим, яке містить обов'язок роботодавців забезпечувати прозорість щодо збору та використання персональних даних;
- правом доступу до даних про працівників, котрі роботодавець зберігає;
- правом на виправлення недостовірних або неповних даних;

- правом видаляти дані про працівників, які зберігає роботодавець;
- правом блокувати або припиняти обробку персональних даних за певних обставин;
- правом отримувати та використовувати персональні дані для власної потреби (знову ж таки за певних обставин).

Для мети цього Регламенту персональними даними вважають будь-які відомості, які стосуються ідентифікованої особи чи придатної до ідентифікації фізичної особи. Ідентифікованою, зі свого боку, буде фізична особа, яку можна визначити безпосередньо чи опосередковано, зокрема, за посиланням на такий ідентифікатор, як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або один чи більше факторів специфічної для фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї фізичної особи.

З урахуванням наведеного можна констатувати, що кожен роботодавець обробляє персональні дані всіх своїх працівників. Наприклад, їх імена, адресу інформацію, контактні дані, номери банківських рахунків та дані про зарплату. Необхідність їхньої обробки очевидна, а в окремих випадках – навіть обов'язкова. Зокрема, роботодавці зобов'язані вести облік днів тимчасової непрацездатності працівників із метою правильного нарахування оплати праці. Так само, як і реквізити банківських рахунків працівників потрібні для виплати їхнього заробітку. Або ж із метою оподаткування – реєстраційні номери працівників як платників податків. Без цієї інформації роботодавець не зможе реалізувати свої обов'язки за трудовим договором.

Окрім цієї мінімальної частини даних, які обробляються роботодавцями, щодня вони можуть автоматично накопичувати відомості про працівників за результатами використання ними цифрового обладнання та завантажених на них додатків, котрі надаються роботодавцем (електронні листи, календарі, стандартні журнали тощо). Деякі роботодавці цілеспрямовано обробляють особисті дані працівників, отримані за допомогою різноманітних технологій моніторингу чи спостереження. Це, наприклад:

- зображення камери або записи відеоспостереження;
- інформація про використання Інтернету та електронної пошти;
- записи телефонних дзвінків або обміну миттєвими повідомленнями;
- інформація про використання мобільних пристроїв, таких як телефони та ноутбуки;
- дані про відстеження або місце розташування автомобілів чи іншого обладнання роботодавця.

Незважаючи на такий широкий перелік потенційно потрібних відомостей, Регламент (ЄС) 2016/679 наголошує, що збір інформації щодо працівника повинен обмежуватись даними, котрі є необхідними та доречними з огляду на обсяг трудових прав та обов'язків особи.

Обробку персональних даних працівників як складника їх приватності роботодавець може здійснювати лише в разі фактичної необхідності та за наявності достатніх правових підстав.

За загальним правилом, найпоширенішим та найважливішим правовим підґрунтям для обробки персональних даних є згода особи, однак це правило не діє

щодо трудових відносин. Фінансова та дисциплінарна залежність працівника від роботодавця може поставити під сумнів дійсність його волевиявлення на обробку [3, с. 23]. Тому, оцінюючи дійсність згоди в контексті працевлаштування, потрібно уважно аналізувати умови, за яких запитується така згода.

Крім цього, в разі незгоди працівника на обробку персональних даних виникає реальне або потенційне упереджене ставлення до нього. З огляду на це роботодавці повинні обґрунтовувати це іншими юридичними підставами. Відповідно до Регламенту (ЄС) 2016/679, крім згоди працівника, юридичною основою для обробки персональних даних працівників може бути необхідність:

- виконання умов трудового договору чи підготовка до його укладення;
- дотримання юридичного зобов'язання;
- захист життєвих інтересів працівника чи іншої фізичної особи;
- виконання завдання в інтересах суспільства або для здійснення публічних повноважень;
- законний інтерес роботодавця.

Правила обробки персональних даних у сфері працевлаштування повинні містити чіткі заходи щодо захисту людської гідності, законних інтересів та основоположних прав працівників [3, 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 входні 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 [4, с. 237].

У цьому контексті на рівні Європейського Союзу 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 [3, с. 16].

Чи не найбільш проблемним є автоматизований моніторинг. Розпізнавання рис та міміки обличчя працівників, як правило, вважається незаконним. Так само

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.

Сама ж обробка повинна бути не лише чесною та прозорою щодо працівників, але також пропорційною меті збору інформації. Роботодавець повинен гарантувати, що будь-які результати моніторингу працівників використовуються виключно для тієї мети, для якої вони отримані. Наприклад, результати моніторингу, котрі використовуються для виявлення та запобігання порушень безпеки даних або для виявлення та запобігання шахрайству, не можуть використовуватись для оцінки працездатності працівників. А рішення щодо ефективності роботи працівників або щодо умов їх працевлаштування ніколи не можуть прийматись виключно на підставі даних автоматизованої обробки чи моніторингу.

Кожен роботодавець повинен володіти достатніми аргументами для підтвердження необхідності та пропорційності обробки персональних даних. Це означає, що він мусить виконувати лише ті операції з обробки, які можуть досягти поставленої мети за найменшого втручання у приватне життя працівника. Ураховуючи наведене, не буде законною діяльність роботодавця щодо збору та обробки персональних даних працівника, котрі він оприлюднив через соціальні мережі. Для обробки відповідних персональних даних вимагається правове підґрунтя, наприклад, таке, як законний інтерес. У цьому контексті роботодавець, перш ніж перевірити профіль особи в одній із соціальних мереж, повинен упевнитись, чи висвітлена інформація має професійний характер, чи такий, який стосується приватного життя особи. Інакше правова допустимість такої його діяльності може бути поставлена під сумнів. Водночас роботодавці зобов'язані утриматись від запровадження вимоги про надання їм доступу до профілю працівника в соціальних мережах, де особа оприлюднює інформацію про себе.

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 працівни-

ків. Належним чином засвідчена поінформованість працівника про регулярність вивчення роботодавцем його публічних дописів є ще однією умовою законності здійснення відповідного моніторингу [3, 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 [5, 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.

Новим також є закріплений Регламентом (ЄС) 2016/679 механізм реалізації «права бути забутим», якщо працівник вимагає цього¹.

Регламент (ЄС) 2016/679 зобов'язує власників баз персональних даних вжити спеціальних заходів із метою дотримання процедури захисту відповідної інформації. Зокрема, вони повинні призначити спеціально уповноважену особу з питань обробки персональних даних, за певних умов.

Згідно зі статтею 88 Регламенту державам-членам Європейського Союзу надаються повноваження встановлювати більш чіткі правила щодо захисту персональних даних працівників шляхом ухвалення спеціальних національних законів або ж погодження відповідних положень у колективних договорах. Зокрема, в такий спосіб можуть бути уточнені правила обробки даних із метою набору персоналу, виконання трудового договору, організаційно-управлінської діяльності у сфері найманої праці, забезпечення єдності та диференціації на робочому місці, забезпечення професійної безпеки та охорони здоров'я працівників на робочому місці, захисту майна роботодавця чи його контрагентів, а також із метою реалізації індивідуальних та колективних трудових прав, зокрема права на припинення трудових правовідносин.

Важливою новелою Регламенту (ЄС) 2016/679 є зміна підходів щодо штрафних санкцій за порушення правил безпеки персональних даних. Зокрема, фрагментарну систему заходів примусу було замінено на грошові штрафи за порушення в цій сфері та одночасно запроваджено механізми невідворотності та послідовності призначення покарання. Суттєві штрафи за порушення правил безпеки персональних даних не лише стимулюють невідворотність покарання, вони є помітною особливістю Регламенту (ЄС) 2016/679, яка змусить національні та транснаціональні компанії інвестувати більше ресурсів у системи та механізми безпеки [7, с. 168].

Наслідки введення в дію Регламенту (ЄС) 2016/679 у сфері захисту персональних даних працівників зможуть оцінити не лише роботодавці держав-членів ЄС, але і їхні партнери із третіх держав. Адже його положення підлягають застосуванню також до компаній не з країн-членів ЄС, які працюють із контрагентами та/або клієнтами із країн-членів ЄС.

¹ «Право бути забутим» означає можливість працівника в певних випадках вимагати видалення всіх своїх даних, якими володіє роботодавець [6].

Висновки. Унаслідок проведеного аналізу можна ствердити, що у ЄС до забезпечення балансу інтересів роботодавців та працівників під час обробки персональних даних останніх можна наблизитись, якщо відповідна обробка відповідатиме таким вимогам:

- буде адекватною, доречною та обмежуватиметься досягненням необхідної мети;
- використання, мета та спосіб обробки повинні бути зрозумілі для працівників;
- працівники повинні мати можливість реалізувати свої права перевіряти, виправляти, припиняти та обмежувати обробку;
- персональні дані повинні зберігатись не більше, ніж потрібно;
- персональні дані повинні бути захищені відповідними технічними та організаційними заходами безпеки.

Література

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *OJ L*. 119, 4.5.2016. P. 1–88.
2. De Hert P.-Papakonstantinou V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law and Security Review*. 2016, Vol. 32, № 2, Pages 179–194.
3. WP29, 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>.
4. Яворська І., Микієвич М. Захист персональних даних у праві Європейського Союзу. *Вісник Львівського університету. Серія міжнародні відносини*. 2019. Випуск 46. С. 234–240.
5. Ogrisek C., GDPR and Personal Data Protection in the Employment Context. *Labour and Law Issues*. 2017. Vol. 3. № 2. 24 p.
6. Pirkova L., Masse E., EU Court decides on two major “right to be forgotten” cases: there are no winners here (23 October 2019). URL: <https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/>.
7. Шевчук О. Правове регулювання охорони персональних даних в Європейському Союзі : дис. ... канд. юрид. н. : спец. 12.00.11 – міжнародне право. Київ, 2018. 197 с.

Анотація

Рим О. М. Захист персональних даних працівників у Європейському Союзі. – Стаття.

У статті аналізуються правові засади системи захисту персональних даних працівників у Європейському Союзі. Проаналізовано права працівників у зв'язку з обробкою їхніх персональних даних роботодавцями, визначено поняття таких даних. Зазначається, що, незважаючи на широкий перелік потенційно потрібних роботодавцю відомостей про працівника, збір відповідної інформації повинен обмежуватись даними, котрі є необхідними та доречними з огляду на обсяг трудових прав та обов'язків особи. Автор акцентує увагу на тому, що обробку персональних даних працівників як складника їх приватності роботодавець може здійснювати лише в разі фактичної необхідності та за наявності достатніх правових підстав. Зокрема, юридичною основою для обробки персональних даних працівників може бути необхідність виконання умов трудового договору чи підготовка до його укладення, дотримання юридичного зобов'язання, захист життєвих інтересів працівника чи іншої фізичної особи, виконання завдання в інтересах суспільства або для здійснення публічних повноважень, а також законний інтерес роботодавця. З'ясовуються питання захисту персональних даних дистанційних працівників та правила використання інформації, яка отримана завдяки автоматизованим системам спостереження на робочому місці. Наголошується, що обробка персональних даних повинна бути чесною та прозорою щодо працівників, а також пропорційною меті збору інформації. Роботодавець повинен гарантувати, що будь-які результати моніторингу працівників використовуються лише для тієї мети, для якої вони отримані. Аналізується допустимий порядок збирання персональних даних та їх обробки. У цьому контексті важливе значення відводиться процедурі надання згоди працівника на обробку його персональних даних. Оцінюючи дійсність згоди в контексті працевлаштування, потрібно уважно аналізувати умови, за яких запитується така згода. Пояснюються способи реалізації зобов'язання роботодавця

інформувати працівників про те, яку інформацію про них він може обробляти, як буде здійснюватись ця обробка та якими правами працівники володіють щодо захисту власної приватності. Підсумовується, що правомірною вважатиметься обробка персональних даних працівників, котра буде адекватною, доречною та обмежуватиметься досягненням необхідної мети, а також якщо використання, мета та спосіб обробки будуть зрозумілі працівникам.

Ключові слова: трудові відносини, конфіденційність, роботодавець, моніторинг на робочому місці, право бути забутим.

Summary

Rym O. M. Employee's personal data protection in European Union. – Article.

The article outlines the system of personal data protection of employees in the European Union. The rights of employees in connection with the processing of their personal data by employers are analyzed, the concept of such data is defined. It is pointed out that despite the wide range of potentially necessary information about the employee, the collection of relevant information by employer should be limited to data that are necessary and relevant to the scope of labour rights and duties of the employee. The author emphasizes that the processing of personal data of employees as part of his privacy can be conducted by employer only if necessary and if there are sufficient legal grounds. In particular, the legal basis for the processing of personal data of employees may be the need to perform the employment contract or preparation for its fulfillment, compliance with legal obligations, protection of vital interests of the employee, or another individual, public interest or legitimate interest of employer. The issues of protection of personal data of remote workers and the rules of use of information obtained through automated surveillance systems in the workplace are outlined. It is emphasized that the processing of employees' personal data must be fair and transparent as well as proportionate to the purpose of collecting information. Employer must ensure that any results of employee monitoring are used exclusively for the purpose for which they were obtained. The admissible order of personal data collection and their processing is analyzed. In this context, the procedure of obtaining the employee's consent to the processing of his data is of great importance. In assessing the validity of consent in the context of employment, the conditions under which such consent is requested should be carefully analyzed. It is explained how to fulfill employer's obligation to inform employees of the types of information he can process about them, how this processing will be performed, and what rights employees have to protect their privacy. It is summarized that the processing of personal data of employees will be considered lawful if it is adequate and limited to achieving the necessary objectives, as well as if the use, purpose, and method of processing will be understood by employees.

Key words: labour relations, employer, monitoring at the workplace, the right to be forgotten.