УДК 341.171

Дейкун Ірина Володимирівна –
студентка 1 курсу магістратури
Інституту підготовки кадрів для органів юстиції України
Національного юридичного університету імені Ярослава Мудрого

Iryna V. Deikun –
1st year Master's student of
Personnel Training Institute for the Bodies of Justice of Ukraine
Yaroslav Mudryi National Law University
(77 Pushkinska Street, Kharkiv, 61024, Ukraine)

Становлення та розвиток медіації у вирішенні трудових спорів: досвід зарубіжних країн GDPR чи Закон України «Про захист персональних даних» - що ефективніше?

У статті проаналізовано основні положення Регламенту General Data Protection Regulation у контексті порівняння з Законом України «Про захист персональних даних». Визначено переваги Регламенту та необхідність прийняття нового Закону в Україні, який би регулював захист персональних даних на європейському рівні.

Ключові слова: *персональні дані, захист персональних даних, регламент, cookie, контролер, процесор, користувачі, комісія, адекватність захисту.*

В статье проанализированы основные положения Регламента General Data Protection Regulation в контексте сравнения с Законом Украины «О защите персональных данных». Определены преимущества Регламента и необходимость принятия нового Закона в Украине, который бы регулировал защите персональных данных на европейском уровне.

Ключевые слова: *персональные данные, защита персональных данных, регламент, cookie, контроллер, процессор пользователи, комиссия, адекватность защиты.*

I.V. Deikun GDPR or On Protection of Personal Data – What is More Efficient?

The article has analyzed the main provisions of General Data Protection Regulation and compared it with the Law of Ukraine 'On Data Protection'. Advantages of the Regulation and necessity to adopt a new Law of Ukraine which could regulate data protection on European level have been identified.

The main provisions which are necessary to be implemented in future legal act have been defined. They are the following: personal data, controller, data processor, adequacy of protection etc. It is also necessary to identify rights, obligations, functions, competence and goal of activities after implementing such notions as controller and processor.

An important aspect is fines for violation of legislation on personal data protection. The Regulation provides for several types of violations and fine sanctions for them. Liability for violation of standards in the sphere of personal data protection ensures an effective mechanism for implementation of Regulation.

The article has also analyzed the notion 'adequacy of protection'. The list of sources which were checked on 'adequacy' has been identified. The main criteria of 'adequacy' which the state has to comply with have been specified. The term for undergoing the inspection regarding compliance with 'adequacy of protection' has been defined. Criteria which the states should comply with in order to undergo the inspection have been provided.

It is also necessary to define the mechanism for control in the sphere of personal data protection. The Regulation provides clear criteria for existence of this mechanism which should be implemented not only on the territory of Ukraine.

Existing provisions of the Law have been analyzed. Compared analysis of the term 'privacy policy' has been done and gaps in Ukrainian legislation have been studied. Compliance of the Regulation with a standard Ukrainian consent for processing of personal data has been defined.

Keywords: *personal data, personal data protection, Regulation, cookie, controller, processor, users, commission, adequacy of protection.*

Постановка проблеми. Сучасні суспільні відносини характеризуються широким використанням персональних даних під час обігу інформації, товарів, послуг і капіталів, що вимагає не тільки вільного руху інформації про особу, а й забезпечення її надійного захисту відповідно до основних прав і свобод людини. На сьогодні інформація про особу та забезпечення захисту цієї інформації потребує неабиякої уваги, передусім з точки зору змісту таких понять, як персональні дані, ідентифікаційний номер та ідентифікація даних. З прийняттям у 2018 році Регламенту General Data Protection Regulation світ заговорив про необхідність правильно зберігання персональних даних.

Аналіз останніх досліджень і публікацій. Дану тематику досліджували такі українські вчені як В. Б. Авер'янова, С. С. Алексєєва, Г. Л. Акопова, І. Л. Бачило, В. М. Брижка, О. А. Банчука, С. Ф. Гуцу, В. І. Гурковського, А. М. Гулеміна, Н. В. Паршиної, В. С. Цимбалюка, І. В. Мартьянова, О. В. Синєокого також зарубіжні У. Просер, Ч. Рааб, С. Стремхолм, У. Фрідман, Л. Шойом, Р. Уекс та інші.

Невирішні раніше проблеми. Надання порівняльної характеристики українським правилам з європейськими стандартами з метою вдосконалення національних норм. Реформування цих стандартів дозволить наблизити українське законодавство до європейських стандартів.

Мета. Надати порівняльну характеристику Закону України «Про захист персональних даних» з новими європейськими стандартами захисту персональних даних, які містяться в General Data Protection Regulation.

Виклад основного матеріалу. Після набрання чинності 25 травня 2018 року Регламенту General Data Protection Regulation (далі – «GDPR» або «Регламент») світ заговорив про нові правила захисту персональних даних. Цей Регламент замінив існуючу на той момент Директиву Європейського Парламенту 95/46/ЄС та Ради «Про захист фізичних осіб при обробці персональних даних та про вільне переміщення цих даних». Положення Регламенту встановлюють нові європейські стандарти захисту персональних даних. Метою GDPR є надання громадянам та резидентам Європейського Союзу контроль за їхніми персональними даними, а також спрощення регуляторного середовища для міжнародного бізнесу [1].

Ст. 2 Закону України «Про захист персональних даних» (далі -Закон) визначає, що персональні дані – це відомості чи сукупність відомостей про фізичну особу , яка ідентифікована або може бути конкретно ідентифікована. GDPR містить інше визначення персональних даних, а саме – це будь-які дані, які прямо чо опосередковано дозволяють встановити особу [5]. До таких даних відноситься не лише ім'я, прізвище телефонний номер або e-mail, але і cookie-файли, а також дані систем Інтернет-статистики чи реклами. Зокрема п. 30 Регламенту визначає, що фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, зокрема IP-адрес, ідентифікаторів «cookie» (реп'яшків) або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації. Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації [1].

З метою зменшення ризиків для відповідних суб'єктів даних та допомогти контролерам і операторам у виконанні своїх обов'язків із захисту даних п 28 закріплює використання суб'єктами псевдонімів. Слід зауважити, що в українському Законі такого положення не зазначено.

Дія GDPR поширюється на будь-яку компанію, яка пропонує користувачам, які знаходяться на території ЄС товари та послуги чи ведуть моніторинг дій. Під останньою дією мається на увазі будь-які компанії, які мають веб-

сайт, користувачі якого знаходяться на території ЄС.

Одним з переваг GDPR є вимога «contact point» з суб'єктом персональних даних, який має право відзиву згоди на обробку персональних даних, яку дав раніше, також подати запит і отримати свої данні, які зберігаються організацією, отримання результатів інформації про цілі та результат обробки персональних даних, видалити ці дані або внести в них зміни, якщо були знайдені неточності [1].

Слід відмітити, що персональні дані можуть зберігатися як з ідентифікацією певної особи, так і анонімно. У останньому випадку комунікація між зберігачем даних та особою не обов'язкова.

Однією з важливих переваг Регламенту є те, що за неправильне поводження з персональними даними особа може нести відповідальність. Регламент закріплює такі види санкцій: попередження в письмовій формі, регулярні періодичні перевірки захисту даних, два види штрафу (до 10 млн євро або 2% річного обороту коштів минулого року організації та 20 млн. євро або 4% від річного обороту коштів минулого року організації. Застосовуватися буде вищий розмір).

В українському нормативно-правовому акті таких положень не передбачено. Також відсутній механізм перевірки порушень зберігання персональних даних.

Регламент закріпив два шляхи механізму виявлення порушень GDPR: скарга та перевірка. Скаргу подає сама особа до зберігача даних. Досить розповсюдженою є ситуація серед європейських користувачів, коли користувач отримує повідомлення з розсилки, на яку не підписувався.

Перевірка може проходити в різних формах. Один з найпростіших це пройти шлях реєстрації користувача сайту.

Одним з нововведень GDPR є звітність про процес обробки персональних даних. Також, у випадку втрати даних або надходження інформації щодо неправомірного використання, зберігач має повідомити особу протягом 72 год. У випадку втрати, необхідно повідомити через представника ЄС регулятора і зазначити причину і який саме обсяг даних втрачено. Також повідомити про заходи, які вживаються для усунення або зменшення наслідків.

Важливою перевагою GDPR над Законом є також розподіл повноважень при процесі обробки, зберігання та видалення персональних даних. Зокрема, з'явилися такі поняття як контролер (data controller)та процесор (data processor). Контролер виконує керуючу функцію над процесором, а саме вказує останньому на порядок та правильність обробки персональних даних. Процесор виконує функцію виконавця, тобто виконує всі процеси, які необхідні для збереження персональних даних.

Регламент запровадив таке поняття як «адекватність» рівня захисту персональних даних. У цьому плані GDPR не принесе ніяких спрощень, а навпаки, для отримання оцінки «адекватності» необхідно відповідати критеріям, передбаченим ст. 45 Регламенту, вони поділені на три категорії. До першої належать: верховенство права, повагу до прав людини та фундаментальних свобод, відповідне законодавство, як загальне, так і секторальне, в тому числі щодо громадської безпеки, оборони, національної безпеки та кримінального права і доступу органів публічної влади до персональних даних, а також імплементацію такого законодавства, норми про захист даних, правила професійної діяльності та заходи з безпеки, в тому числі, правила для наступного передавання персональних даних до іншої третьої країни чи міжнародної організації, яких дотримуються в такій країні чи міжнародній організації, судову практику, а також дієві права суб'єкта даних, які можна реалізувати, та дієвий адміністративний і судовий захист для суб'єктів даних, чиї персональні дані передають [1].

До другої: існування та дієве функціонування незалежних наглядових органів у третій країні чи тих, яким підпорядковується міжнародна організація, із відповідальністю за забезпечення та дотримання норм про захист даних, у тому числі, належними правозастосовними повноваженнями, для надання допомоги та рекомендацій суб'єктам даних під час реалізації їхніх прав і для співпраці з наглядовими органами держав-членів [1].

До третьої, міжнародні зобов'язання, що взяли на себе третя країна або відповідна міжнародна організація, або інші зобов'язання, що випливають із юридично зобов'язальних конвенцій або інструментів, а також із їхньої участі в багатосторонніх або регіональних

системах, зокрема в сфері захисту персональних даних. Рівень «адекватності» буде переглядатися кожні 4 роки [1].

Станом на 25 січня 2019 Комісія ЄС зробила висновки про адекватність щодо наступних країн і територій: Андорра, Аргентина, Канада (комерційні організації), Фарерські острови, Гернсі, Ізраїль, острів Мен, Джерсі, Нова Зеландію, Швейцарія, Уругвай і Сполучені Штати Америки (обмежена рамками EU-US Privacy Shield framework), Японія (рішення від 23 січня 2019). Визначення адекватності для Канади охоплює тільки ті дані, які підпадають під дію Канадського закону про захист персональних даних і електронних документів (Canada's Personal Information Protection and Electronic Documents Act, або PIPEDA) [4].

Значним досягненням Регламенту є введення корпоративних правил, що передбачені ст. 47 (BCRs). Ці корпоративні правила зобов'язують визначати:

- структуру та контактні дані групи підприємств, що здійснюють спільну господарську діяльність;
- передавання даних чи низку актів передавання, утому числі категорії персональних даних, тип опрацювання і його цілі, тип суб'єктів даних, що зазнали впливу та визначення відповідної третьої країни чи країн;
- їхню обов'язкову юридичну природу, як внутрішню, так і зовнішню;
- процедури подання скарг і т д [1].

Перевагами BCRs є зменшення адміністративної тяганини і робіт у співвідношенні транскордонних переміщень, чітка структура зберігання персональних даних, дотримання принципів захисту даних і т д.

Регламентом чітко розмежовано поняття Privacy Policy та Privacy Note. Перший документ встановлює правила збору і обробки персональних даних користувачів на певному веб-ресурсі. Privacy Note направлений суб'єктам персональних даних, де власник персональних даних вказує, яким чином він збирає, використовує, передає персональні дані.

Український законодавець закріпив поняття Privacy Policy, але не приділив уваги Privacy Note. Український варіант Privacy Policy значно відрізняється від європейського. Натискання на кнопку «я згоден» допускається Регламентом лише в деяких випадках. Виконання вимог ч. 2 ст. 7 GDPR «якщо суб'єкт даних надає згоду в контексті письмової декларації, що також стосується інших питань, запит на надання згоди необхідно подавати у формі, що чітко відрізняється від інших питань, у зрозумілій та доступній формі, з використанням чітких і простих формулювань. Будь-яка частина такої декларації, що становить порушення цього Регламенту, не є зобов'язальною».

Отже, положення Закону України «Про захист персональних даних» значно поступаються європейським стандартам. Для досягнення максимального рівня якості захисту національному законодавцю необхідно розробити новий нормативно-правовий акт, положення якого будуть відповідати європейським нормам. Для цього необхідно закріпити базові поняття такі як: контролер, процесор і т д. Визначити необхідними у використанні Privacy Policy та Privacy Note. Надати нове сучасне поняття «персональних даних». Пройти процес адекватності Комісією ЄС. Необхідно закріпити юридичну відповідальність за неправильне зберігання персональних даних, а також процедуру притягнення до неї.

Список використаних джерел:

1. 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): 2015. URL: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.
2. Имеет ли GDPR отношение к Вам? Основные правовые аспекты, которые необходимо знать: 2019. URL: https://www.de-jure.ua/imeet-li-gdpr-otnoshenie-k-vam-osnovnye-pra/.

3. Артем Козлюк. GDPR — новые правила обработки персональных данных в Европе для международного IT-рынка: 2018. URL: https://habr.com/ru/company/digitalrightscenter/blog/344064/.
4. Карелов К.Ю. GDPR та Закон України «Про захист персональних даних»: у чому різниця та яких змін потребує національне законодавство?:2019. URL: http://arbitrium.com.ua/ua/gdpr-i-zu-o-zaschite-personalnyh-dannyh-v-chem-raznica-i-v-kakih-izmeneniyah-nuzhdaetsya-nacionalnoe-zakonodatelstvo.html.
5. Про захист персональних даних: Закон України від 01.06.2010. *Урядовий кур'єр*. 2010. № 122.

References:

1. 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): 2015. URL: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.
2. Ymeet ly GDPR otnoshenye k Vam? Osnovnie pravovie aspekti, kotorie neobkhodymo znat: 2019. URL: https://www.de-jure.ua/imeet-li-gdpr-otnoshenie-k-vam-osnovnye-pra/.
3. Artem Kozliuk. GDPR — novie pravyla obrabotky personalnikh dannikh v Evrope dlia mezhdunarodnoho IT-rinka: 2018. URL: https://habr.com/ru/company/digitalrightscenter/blog/344064/.
4. Karelov K.Yu. GDPR ta Zakon Ukrainy "Pro zakhyst personalnykh danykh": u chomu riznytsia ta yakykh zmin potrebuie natsionalne zakonodavstvo?:2019. URL: http://arbitrium.com.ua/ua/gdpr-i-zu-o-zaschite-personalnyh-dannyh-v-chem-raznica-i-v-kakih-izmeneniyah-nuzhdaetsya-nacionalnoe-zakonodatelstvo.html.
5. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010. *Uriadovyi kur'ier*. 2010. № 122.