УДК 347.421

DOI <https://doi.org/10.32844/2618-1258.2019.2-1.10>

ВЕРЕС І.Я.

ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У ДОГОВІРНИХ ЦИВІЛЬНО-ПРАВОВИХ ВІДНОСИНАХ

У науковій статті досліджені умови правомірного використання персональних даних у договірних відносинах. Використання персональних даних можливе лише з метою належного виконання договору. Обсяг персональних даних має бути необхідним та достатнім для використання в договірних відносинах. Здійснення передачі персональних даних третім особам можливе лише за згодою особи. Винятком може бути ситуація, коли персональні дані боржників можуть бути передані без їхньої згоди в разі заміни кредитора у зобов'язанні. Особа здійснює також контроль за використанням її персональних даних після укладення договору або надання згоди на використання третім особам. Зокрема, вона має право 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 нею особам, крім випадків, встановлених законом, тощо. Використання персональних даних можливе за умови створення умов для захисту. Умовно заходи можна поділити на технічні та організаційні. Технічними заходами забезпечення безпеки опрацювання даних є, зокрема, використання псевдонімів і шифрування персональних даних; здатність забезпечувати безперервну конфіденційність, цілісність, наявність та стійкість систем та послуг опрацювання; здатність вчасно відновити наявність і доступ до персональних даних у випадку технічної аварії тощо. Організаційним заходом є створення структурного підрозділу або уповноваження відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних під час їх обробки. Проаналізувавши норми ЗУ «Про захист персональних даних» та Регламенту Європейського Парламенту і Ради (ЄС) про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, слід зазначити, що дані нормативно-правові акти передбачають однакові принципи використання персональних даних, що означає готовність України до вступу в ЄС і поширення дії Регламенту. Однак окремі вимоги Регламенту потребують імплементації в українське законодавство, зокрема, визначення правового статусу контролера, оператора та представника.

Ключові слова: персональні дані, суб'єкт персональних даних, договірні відносини, електронна комерція, захист персональних даних.

The academic article deals with the investigation of conditions of legitimate use of personal data in contractual relations. The Usage of personal data is only possible for the purpose of the proper performance of the agreement. The amount of personal data should be necessary and sufficient for contractual relations. The transfer of personal data to third parties is possible only with the consent of the person. The exception may be that the personal data of the debtors can be transferred without their consent when replacing the creditor in the obligation. The person also controls the use of his personal data after the conclusion of the agreement or giving consent for use to third parties. In particular, it has the right to know about the sources of collection, the location of its personal data, the purpose of their processing, the location or place of residence (stay) of the owner or manager of the personal data, or to give the relevant instruction to receive this information by authorized people, except in cases established by law; etc. The use of personal data is possible if conditions for protection are created. Conditionally measures can be

divided into technical and organizational. Technical measures to ensure the security of data processing are, in particular, the usage of aliases and encryption of personal data; the ability to ensure the continuous confidentiality, integrity, availability and sustainability of processing systems and services; the ability to restore the availability and access to personal data in time in the event of a technical accident; etc. An organizational measure is the creation of a structural unit or the authorization of the responsible person, who organizes work related to the protection of personal data during their processing. Having analyzed the rules of the Law "Personal Data Security" and the Regulations, it should be noted that these normative acts provide the same principles for the use of personal data, which means Ukraine's readiness to join the EU and the extension of the Regulation.

Key words: *personal data, subject of individual data, contractual relationship, e-commerce, personal data security.*

Вступ. Належне використання персональних даних у державі є гарантією захисту прав людини. Україна лише на шляху до формування належної правової бази використання персональних даних. Загальні принципи використання персональних даних визначені в Конституції України, Конвенції про захист людини і основоположних свобод, Закону України (далі – ЗУ) «Про інформацію», ЗУ «Про захист персональних даних», ЗУ «Про електронну комерцію» тощо. Особливо актуальним є врахування правил європейського права про захист персональних даних, зокрема, Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (далі – Регламент) [1]. Окремим питанням використання персональних даних присвячені праці науковців Р.А. Майданика, О.В. Кохановської та інших учених. На сьогодні актуальним є комплексне дослідження нормативно-правової бази України, Регламенту, судової практики та спеціальної наукової літератури, що стосуються використання персональних даних саме в договірних цивільно-правових відносинах.

Постановка завдання. Мета дослідження полягає у формуванні теоретичної концепції використання персональних даних у договірних цивільно-правових відносинах. Для досягнення вказаної мети необхідно дослідити умови використання персональних даних у договірних відносинах, розробити науково обґрунтовані пропозиції, спрямовані на вдосконалення діючого законодавства та правозастосовної практики.

Результати дослідження. Основою положення умовою використання персональних даних у договірних відносинах є те, що використання здійснюється лише з метою належного виконання договору. Підставою для обробки персональних даних стороною правочину є укладення та виконання правочину, стороною якого є суб'єкт персональних даних, або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних (ст. 11 ЗУ «Про захист персональних даних»). П. 44 Регламенту також передбачає, що опрацювання необхідно вважати законним у разі його необхідності для укладення договору або наміру щодо укладення договору.

У ст. 7 Регламенту зазначено, що, здійснюючи оцінку того, чи є згода вільно наданою, необхідно максимально враховувати те, чи залежить, між іншим, виконання договору, в тому числі надання послуги, від згоди на опрацювання персональних даних, що не є необхідною для виконання такого договору. Персональні дані повинні бути достатніми, відповідними та обмежуватися тим, що є необхідним для досягнення цілей, для яких їх опрацьовують. Це вимагає, зокрема, забезпечення того, що період, протягом якого зберігаються персональні дані, був скорочений до абсолютного мінімуму. Персональні дані необхідно опрацьовувати лише тоді, якщо мету опрацювання не можна досягнути іншими засобами. Щоб забезпечити те, що персональні дані не зберігаються довше, ніж це необхідно, контролер повинен установити часові рамки для стирання або періодичного перегляду. Необхідно вживати всіх відповідних заходів для забезпечення виправлення або видалення неточних персональних даних (п. 39 Регламенту).

Важливим питанням є визначення необхідного обсягу персональних даних у договірних відносинах. Особливо це актуально під час укладення договорів у електронній формі. Відповідно до ст. 7 ЗУ «Про електронну комерцію» продавець (виконавець, постачальник) товарів, робіт, послуг в електронній комерції під час своєї діяльності та у разі поширення комерційного електронного повідомлення зобов'язаний забезпечити прямий, простий, стабільний доступ ін-

ших учасників відносин у сфері електронної комерції до такої інформації: повне найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи – підприємця; місцезнаходження юридичної особи або місце реєстрації та місце фактичного проживання фізичної особи – підприємця; адреса електронної пошти та/або адреса інтернет-магазину; ідентифікаційний код для юридичної особи або реєстраційний номер облікової картки платника податків для фізичної особи – підприємця, або серія та номер паспорта для фізичної особи – підприємця, яка через свої релігійні переконання відмовилася від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомила про це відповідний орган державної податкової служби і має відмітку в паспорті; відомості про ліцензування (серія, номер, строк дії та дата видачі), якщо господарська діяльність підлягає ліцензуванню; щодо включення податків у розрахунок вартості товару, роботи, послуги та в разі доставки товару – інформація про вартість доставки; інші відомості, що відповідно до законодавства підлягають оприлюдненню. Відповідно до ст. 8 ЗУ «Про електронну комерцію» покупець (замовник, споживач) товарів, робіт, послуг у сфері електронної комерції, який приймає (акцептує) пропозицію іншої сторони щодо укладення електронного договору, зобов'язаний повідомити про себе інформацію, необхідну для його укладення. У разі оплати вартості товару, роботи, послуги із застосуванням платіжних інструментів така особа має право повідомити відомості, що дають змогу забезпечити проведення оплати відповідним оператором платіжних систем, який несе відповідальність за їх збереження та використання в порядку, передбаченому законодавством. Щодо покупця – фізичної особи, відповідно до ст. 8 ЗУ «Про електронну комерцію», вона повинна надати інформацію про себе, необхідну для вчинення електронного правочину, створення електронного підпису, ідентифікації в інформаційній системі суб'єкта електронної комерції, шляхом введення (створення) особою спеціального набору електронних даних, а також вчинення інших дій у такій системі. Проаналізувавши дані законодавчі положення, слід акцентувати увагу на тому, що законодавець максимально захищає інтереси покупця (замовника, споживача). Законом передбачено розширений перелік персональних даних продавця (виконавця, постачальника) та положення, що продавець (виконавець, постачальник) має право вимагати від іншої сторони лише такі відомості, без яких укладення та виконання зобов'язань за електронним договором неможливе (ч. 4 ст. 7 ЗУ «Про захист персональних даних»). Дані законодавчі положення вважаємо обґрунтованими, оскільки вони зумовлені ризиковістю укладення договору в електронній формі без особистої участі сторін.

Обов'язкове повідомлення персональних даних у договірних відносинах слід розглядати як вимогу закону для забезпечення стабільності цивільного обороту. Однак укладення договору ґрунтується на реалізації принципу «свобода договору» (сторони є вільними в укладенні договору згідно зі ст. 627 ЦК України). Тому, за загальним правилом, використання персональних даних у договірних відносинах здійснюється за згодою особи, при цьому обсяг даних може бути визначено або законом, або за домовленістю сторін договору.

Слід зазначити, що повідомлення персональних даних під час укладення договору не означає припинення режиму конфіденційності, тому будь-яке подальше її використання повинно здійснюватися лише за згодою особи. Тому другою важливою умовою використання персональних даних у договірних відносинах є здійснення передачі персональних даних третім особам за згодою особи. Відповідно до ст. 2 ЗУ «Про захист персональних даних» третя особа – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, який володільцем чи розпорядником персональних даних здійснюється передача персональних даних. Згідно зі ст. 4 Регламенту «третя сторона» означає фізичну чи юридичну особу, орган публічної влади, агентство чи орган, який не є суб'єктом даних, контролером, оператором та особами, які під безпосереднім керівництвом контролера або оператора уповноважені опрацьовувати персональні дані. Згода суб'єкта персональних даних – це 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. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки (ст. 2 ЗУ «Про захист персональних даних»). «Згода» суб'єкта даних означає будь-яке вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта, яким він або вона, шляхом оформлення заяви

чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних (ст. 4 Регламенту).

У судовій практиці є багато справ про розголошення персональних даних однією зі сторін правочину. Значна кількість стосується укладення стороною договору про уступку права вимоги відповідно з передачею інформації про особу боржника новому кредитору.

ТОВ «Арка Капітал Україна» звернулося до господарського суду м. Києва з позовом до ТОВ «Юридична фірма «Ілляшев та партнери», в якому просить зобов'язати відповідача припинити дії, що порушують право позивача в частині розповсюдження без його згоди конфіденційної інформації за договором про надання юридичних послуг. З тексту рішення випливає, що між Позивачем та Відповідачем був укладений договір про надання юридичних послуг, згідно з яким відповідач повинен був надати послуги, а позивач їх оплатити. Відповідно до умов договору текст документа та вся інформація, що надається в межах договору, є конфіденційною. Відповідач уклав договір уступки права вимоги з третьою стороною. Відповідно до умов договору уступки та ч. 1 ст. 517 ЦК України, в разі уступки права вимоги первісний кредитор повинен передати новому кредитору документи на підтвердження існуючої заборгованості. 22.04.2010 р. Рішенням суду позовні вимоги задоволені частково. Відповідача зобов'язано «припинити дії, що порушують право позивача в частині розповсюдження без його згоди конфіденційної інформації за договором про надання юридичних послуг». 07.06.2010 р. Київський апеляційний господарський суд у постанові за результатами розгляду апеляційної скарги погодився з рішенням суду першої інстанції та лишив його в силі [2].

В іншій справі «Південно-Західна залізниця» звернулася до господарського суду м. Києва з позовом до ТОВ «Залізний кулак» про визнання договору недійсним. Судом встановлено, що між Позивачем та Відповідачем укладено договір охорони об'єктів Позивача. Сторони погодили в договорі, що текст договору, будь-які матеріали, інформація та відомості, які стосуються договору, є конфіденційними і не можуть передаватися третім особам без попередньої письмової згоди іншої сторони договору, крім випадків, коли таке передавання пов'язане з одержанням офіційних дозволів, документів для виконання договору або сплати податків, інших обов'язкових платежів, а також у випадках, передбачених чинним законодавством, яке регулює зобов'язання сторін по договору. Відповідач уклав договір з третьою особою про відступлення прав вимоги за договором охорони, відповідно до якого до нового кредитора перейшли права вимоги до позивача за договором охорони. Позивач просить суд визнати укладений договір уступки недійсним на підставі того, що відповідачем не було отримано попередню згоду позивача на передачу новому кредитору будь-яких матеріалів, інформації та відомостей, які стосуються договору. Суд зауважує, що діюче законодавство не пов'язує можливість визнання недійсним договору відступлення права вимоги з обставинами розголошення або нерозголошення конфіденційної інформації за зобов'язаннями, в яких здійснюється заміна кредитора. 21.09.2015 року суд ухвалив рішення, в якому відмовив у задоволенні позову. Дане рішення залишено без змін Постановою Київського апеляційного господарського суду від 03 листопада 2015 року та Постановою Вищого господарського суду України від 23 грудня 2015 року [3]. Суд не визнав порушення закону в діях банку, що передав персональні дані клієнта-боржника товариству, що спеціалізується на колекторській діяльності [4]. З огляду на зміст укладеного договору суди дійшли висновку, що, уклавши цей кредитний договір, особа надала банку свою згоду збирати, зберігати, використовувати, поширювати і отримувати інформацію – дані про неї, відомі банку або третім особам у зв'язку з укладенням та виконанням договору, в тому числі банківську та комерційну таємницю, необхідну для укладання договорів, у тому числі щодо відступлення права вимоги та переведення боргу. Тому дії банку щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних, не є підставою для притягнення банку до цивільно-правової відповідальності. Останні дві судові позиції є обґрунтованими.

Статтею 512 ЦК України визначені підстави заміни кредитора в зобов'язанні. За однією з таких підстав кредитор у зобов'язанні може бути замінений іншою особою внаслідок передавання ним своїх прав іншій особі за правочином (відступлення права вимоги). Крім того, статтею 516 ЦК України також встановлено, що заміна кредитора в зобов'язанні здійснюється без згоди боржника, якщо інше не встановлено відповідним договором або законом. Зважаючи на те, що дозвіл на передачу персональних даних боржників наданий володільцям баз персональних даних згідно з ЦК України, персональні дані боржників можуть бути передані без їхньої згоди. Слід зазначити, що відповідно до ст. 21 ЗУ «Про захист персональних даних» щодо передачі

персональних даних третій особі володільць персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди, або інше не передбачено законом. Відповідно до Регламенту принципи правомірного та прозорого опрацювання вимагають, щоб суб'єкта даних було проінформовано про наявність операції опрацювання та її цілі. Контролер повинен надавати суб'єкту даних будь-яку подальшу інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, враховуючи конкретні обставини та контекст, що супроводжують опрацювання персональних даних (п. 60).

Гарантією належного використання персональних даних є законодавчо передбачена можливість особи контролювати за використанням персональних даних після укладення договору або надання згоди на використання третім особам. У ст. 8 ЗУ «Про захист персональних даних» передбачені права суб'єкта персональних даних, які забезпечують відповідний контроль за використанням персональних даних, зокрема: право 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, установлених законом; право отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані; право на доступ до своїх персональних даних; право отримувати не пізніше як за тридцять календарних днів із дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних; право пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних; право пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними; право відкликати згоду на обробку персональних даних; знати механізм автоматичної обробки персональних даних тощо. Регламент також передбачає механізми можливого контролю особи за використанням її персональних даних. Суб'єкт даних повинен мати право доступу до персональних даних, які збирають щодо нього, і реалізовувати таке право вільно та через розумні проміжки часу для того, щоб бути обізнаним про законність опрацювання та перевірити її. За можливості контролер повинен бути спроможним надавати віддалений доступ до системи безпеки, яка б забезпечила суб'єкту даних прямий доступ до своїх персональних даних (п. 63). Суб'єкт даних повинен мати право відкликати свою згоду в будь-який момент. Відкликання згоди не повинно впливати на законність опрацювання, що ґрунтувалося на згоді до її відкликання. До надання згоди суб'єкта даних необхідно про це повідомити (ст. 7 Регламенту).

Відповідно до ст. 24 ЗУ «Про захист персональних даних» володільці персональних даних зобов'язані забезпечити захист цих даних від випадкових втрат або знищення, від незаконної обробки, в тому числі незаконного знищення чи доступу до персональних даних. Умовно можна поділити ці заходи на технічні та організаційні. Технічні заходи забезпечення безпеки опрацювання даних запропоновані в Регламенті, зокрема: використання псевдонімів і шифрування персональних даних; здатність забезпечувати безперервну конфіденційність, цілісність, наявність та стійкість систем та послуг опрацювання; здатність вчасно відновити наявність і доступ до персональних даних у випадку технічної аварії; процес для регулярного тестування, оцінювання та аналізу результативності технічних і організаційних заходів для гарантування безпеки опрацювання (ст. 32 Регламенту).

Компанія Facebook була оштрафована на 500 тисяч фунтів стерлінгів (близько 645 мільйонів доларів) британською комісією із захисту даних за участь у скандалі з витоком даних Cambridge Analytica. Facebook потрапив у скандал через те, що британська консалтингова фірма Cambridge Analytica, що працювала на Дональда Трампа на виборах у США 2016 року, неправомірно отримала доступ до особистої інформації 87 мільйонів користувачів Facebook. Генеральний директор Facebook Марк Цукерберг визнав, що в його компанії не досить відповідально поставилися до безпеки, що призвело до неналежного використання персональних даних громадян. Щодо організаційних заходів, то згідно зі ст. 24 ЗУ «Про захист персональних даних» у володільців персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних під час їх обробки. Структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних під час їх обробки: 1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних

даних; 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. Фізичні особи – підприємці, в тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону (ст. 24 ЗУ «Про захист персональних даних»). Однією з новел, яка передбачена у Регламенті, є призначення контролера, оператора та представника. Контролер повинен повідомляти фізичну особу (суб'єкта даних) щодо опрацювання її персональних даних, а також надати інформацію щодо терміну зберігання персональних даних, існування права на відкликання згоди в будь-який момент, права звернення зі скаргами до наглядового органу та ін. Такий суб'єкт даних наділений великим спектром прав, серед них: право на доступ до інформації щодо опрацювання даних, право на виправлення, право на стирання, право на обмеження опрацювання, право на мобільність даних. Оператор повинен опрацьовувати дані від імені контролера, а представник – перебувати в країні ЄС, в якій будуть надаватися послуги або здійснюватися продаж товару. Представник призначається контролером або оператором в письмовій формі. У деяких випадках компанія звільняється від призначення представника, а саме коли обробка здійснюється не на постійній основі, не у великому обсязі стосовно спеціальних категорій даних (расову чи етнічну приналежність, політичні переконання тощо) або опрацювання даних про судимості і кримінальні злочини та, ймовірно, не призведе до виникнення ризику для прав і свобод фізичної особи. Контролери, оператори, представники повинні співпрацювати з наглядовими органами, своєчасно надавати відповіді на запити таких органів. Контролер повинен у разі виявлення будь-якого порушення захисту персональних даних не пізніше 72 годин з моменту виявлення звернутися до наглядових органів. Контролер або оператор повинні відшкодувати будь-яку шкоду, заподіяну особі в результаті опрацювання з порушенням цього Регламенту. Контролера або оператора необхідно звільнити від відповідальності у разі доведення, що вони жодним чином не несуть відповідальності за заподіяну шкоду (п. 146).

Висновки. Умовами правомірного використання персональних даних у договірних відносинах є: використання персональних даних лише з метою належного виконання договору; здійснення передачі персональних даних третім особам лише за згодою особи; контроль особи за використанням персональних даних після укладення договору або надання згоди на використання третім особам; використання персональних даних за умови створення умов для захисту. Проаналізувавши норми ЗУ «Про захист персональних даних» та Регламенту, слід зазначити, що дані нормативно-правові акти передбачають однакові принципи використання персональних даних, що означає готовність України до вступу в ЄС і поширення дії Регламенту. Однак окремі вимоги Регламенту потребують імплементації в українське законодавство, зокрема визначення правового статусу контролера, оператора та представника.

Список використаних джерел:

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС.
2. Рішення Київського апеляційного господарського суду від 07.06.2010 року. URL: www.reyestr.court.gov.ua.
3. Постанова Вищого господарського суду України від 23 грудня 2015 року у справі № 910/17726/15. URL: www.reyestr.court.gov.ua.
4. Постанова Судових палат у цивільних та господарських справах Верховного Суду України від 18 вересня 2013 року у справі № 6-75цс13. URL: www.reyestr.court.gov.ua.