УДК 341.174

ШЕВЧУК О.О.

ПРАВОВЕ РЕГУЛЮВАННЯ ТРАНСКОРДОННОЇ ПЕРЕДАЧІ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

У даній статті досліджуються питання правового регулювання транскордонної передачі персональних даних у Європейському Союзі. Пропонується розглянути основні механізми, що забезпечують належний захист персональних даних у разі транскордонної передачі: передача на підставі рішення про визнання належного рівня захисту, передача даних на підставі іншого механізму забезпечення застосування належних запобіжників, кодекси поведінки й системи сертифікації, юридично зобов'язальні корпоративні правила. Розглядаються особливості передачі даних із Європейського Союзу до США згідно з положеннями угоди «Про захист конфіденційності» та передачі даних за межі Європейської економічної зони.

Ключові слова: *транскордонна передача персональних даних, належні запобіжники, юридично зобов'язальні корпоративні правила, типовий договір, Європейської економічної зона, США, Європейський Союз.*

В данной статье исследуются вопросы правового регулирования трансграничной передачи персональных данных в Европейском Союзе. Предлагается рассмотреть основные механизмы, обеспечивающие надлежащую защиту персональных данных при их трансграничной передаче: передача на основании решения о признании надлежащего уровня защиты, передача данных на основании другого механизма обеспечения применения надлежащих предохранителей, кодексы поведения и системы сертификации, юридически обязывающие корпоративные правила. Рассматриваются особенности передачи данных из Европейского Союза в США в соответствии с положениями соглашения «О защите конфиденциальности» и передачи данных за пределы Европейской экономической зоны.

Ключевые слова: *трансграничная передача персональных данных, соответствующие предохранители, юридически обязывающие корпоративные правила, типовой договор, Европейской экономической зона, США, Европейский Союз.*

The article provides the issues of legal regulation of cross-border transfers of personal data in the European Union. It is proposed to consider the main mechanisms ensuring the proper protection of cross-border transfers of personal data: transfers with an adequacy decision, transfer pursuant to another mechanism ensuring appropriate safeguards, codes of conduct and certification mechanism, legally binding corporate rules. The features of data transfer from the European Union to the USA pursuant to Privacy Shield and the transfer of data beyond the European Economic Area boundaries are noted.

Key words: *cross-border data transfer of personal data, appropriate safeguards, legally binding corporate rules, model clauses, European Economic Area, United States, European Union.*

Постановка завдання. Проблема забезпечення безперешкодного руху персоніфікованої інформації між різними юрисдикціями почала виникати ще на початку 80-х рр. XX ст. Неузгодженість національних підходів до гарантування безпеки під час передачі персональних даних спричинило заборони на передачу персональних даних через кордони та появу бар'єрів для ведення бізнесу у різних країнах. Вирішити цю проблему на національному рівні було неможливо, зважаючи на відмінності національних підходів. Зростаючий транскордонний обмін інформацією вимагав уживання невідкладних заходів на міжнародному рівні. Зусилля, спрямовані на створення

© ШЕВЧУК О.О. – аспірант кафедри порівняльного і європейського права (Інститут міжнародних відносин Київського національного університету імені Тараса Шевченка)

міжнародних стандартів для узгодження національних положень щодо захисту приватності та транскордонної передачі персональних даних, були здійснені Європейським Союзом (ЄС) та такими міжнародними організаціями, як Рада Європи, Організація Економічного Співробітництва та Розвитку (ОЕСР) та Організація Об'єднаних Націй.

Дана стаття ставить за мету виробити комплексний підхід до питання транскордонної передачі персональних даних у Європейському Союзі та дослідити сучасний стан проблематики даного питання.

Питанню транскордонної передачі персональних даних у Європейському Союзі присвячені численні праці вітчизняних та європейських науковців. Дослідженню окремих питань цієї проблематики приділяли увагу такі фахівці, як Анна Майерс, Детлев Гебель, Тім Хікман, Марк Лаббок, Наталіна Флірі, Андреас Марошч, Пабло Гарсія Мехіа.

Результати дослідження. Транскордонні потоки персональних даних необхідні для розширення міжнародної торгівлі та міжнародного співробітництва. Збільшення цих потоків призвело до виникнення нових проблем щодо захисту персональних даних. У разі передачі персональних даних із ЄС у треті країни або міжнародні організації має бути дотриманий певний рівень захисту.

Транскордонна передача персональних даних – це передача персональних даних одержувачу, який знаходиться під іноземною юрисдикцією.

Регламент (ЄС) 2016/679 (далі – Регламент) дозволяє передавати персональні дані третім країнам або міжнародним організаціям у разі виконання ними встановлених умов, у т. ч. щодо подальшої передачі. Будь-яка передача персональних даних, що знаходяться в опрацюванні чи призначені для опрацювання після передачі до третьої країни чи міжнародної організації, відбувається, якщо, з урахуванням інших положень цього Регламенту, оператор і процесор дотримуються умов, у т. ч. для наступних передач персональних даних із третьої країни чи міжнародної організації до іншої третьої країни чи міжнародної організації.

Подібно до системи, передбаченої Директивою 95/46/ЄС, Регламент дозволяє передачу даних до держав, чиє законодавство визнане Єврокомісією здатним забезпечити «належний» рівень захисту персональних даних. Однак, навіть за відсутності висновку про належний рівень захисту, передача даних за межі держав-членів ЄС дозволяється за певних обставин, як-от на підставі положень типового договору або юридично зобов'язальних корпоративних правил (далі – ЮЗКП).

Варто зазначити важливі відмінності між Регламентом та Директивою. Зокрема, Регламент прямо визнає дійсними для оператора та процесора чинні вимоги до ЮЗКП, що сприятиме передачі даних, у яких беруть участь держави-члени, які досі не визнали ЮЗКП. Положення типового договору, які до появи Регламенту потребували попереднього повідомлення співробітника із захисту даних і його схвалення, тепер можуть застосовуватися без такого попереднього схвалення. Окрім того, нова система, запроваджена положеннями ст. 42, дозволяє передавати дані на підставі сертифікації за умови взяття оператором або процесором на себе правових зобов'язань застосування належних запобіжників із можливістю примусу до виконання таких зобов'язань [1].

Передача на підставі рішення про визнання належного рівня захисту. Положення глави V (ст. 44–49) Регламенту регламентують транскордонну передачу персональних даних. Ст. 45 визначаються умови для передачі на підставі рішення про визнання належного рівня захисту [2]; ст. 46 визначаються умови для передачі даних із застосуванням належних запобіжників у випадку відсутності рішення про визнання належного рівня захисту [3]; ст. 47 визначаються умови передачі даних на підставі юридично зобов'язальних корпоративних правил [4]; у ст. 48 ідеться про ситуації видання іноземними судом або адміністративним органом розпорядження про передачу даних, яке в інших випадках не дозволене положеннями Регламенту [5]; нарешті ст. 49 визначаються умови застосування винятків в окремих ситуаціях за відсутності рішення про визнання належного рівня захисту або відсутності належних запобіжників.

Згідно з Директивою, передача персональних даних за межі держав-членів могла здійснюватися лише до схвалених третіх країн. Регламент дозволяє передачу не лише до третіх країн, але також до окремих територій або міжнародних організацій за умови визнання Єврокомісією рівня захисту в них належним. Прийняття (або відкликання) Єврокомісією рішення про визнання належного рівня захисту одразу ж стає юридично зобов'язальним для всіх держав-членів.

Передача даних організації з «належним» рівнем захисту може здійснюватися без додаткових дозволів Єврокомісії або держав-членів. Рішення про визнання належного рівня захисту

підлягають також періодичному перегляді для перевірки систематичності підтримання організацією належного рівня захисту даних. Під час періодичних переглядів Єврокомісія проводить консультації з організацією і враховує актуальні зміни, які в ній відбулися, а також інформацію від інших зацікавлених джерел, як-то Європейського Парламенту або Ради.

Передача даних на підставі іншого механізму забезпечення застосування належних запобіжників. Подібно до Директиви, за відсутності рішення про визнання належного рівня захисту Регламент запроваджує механізми транскордонної передачі даних за умови застосування оператором або процесором певних запобіжників. Згідно з положеннями ст. 49, належними запобіжниками є:

– юридично зобов'язальний документ із можливістю примусу до його виконання, сторонами якого є органи державної влади або державні установи.

– юридично зобов'язальні корпоративні правила відповідно до положень ст. 47.

– положення про захист даних типового договору, затверджені Єврокомісією з дотриманням процедури розгляду, зазначеної в ст. 93 (2).

– схвалений кодекс поведінки згідно з положеннями ст. 40 у поєднанні з правовими зобов'язаннями з можливістю примусу до їхнього виконання, взятими на себе оператором або процесором у третій державі, щодо застосування належних запобіжників, у т. ч. в аспекті дотримання прав суб'єктів даних.

– схвалена система сертифікації згідно з положеннями ст. 42 у поєднанні з правовими зобов'язаннями з можливістю примусу до їхнього виконання, взятими на себе оператором чи процесором у третій країні, щодо застосування належних запобіжників, у т. ч. в аспекті дотримання прав суб'єктів даних [6].

Положення про захист даних типового договору. Зміни, внесені у вимоги щодо положень про захист даних типового договору, зменшують створюване ними адміністративне навантаження. За Регламентом ці положення можуть застосовуватися без попереднього дозволу наглядових органів і затверджуватися Єврокомісією, а також національними наглядовими органами. Чинність існуючих положень типового договору може зберегтися, але Регламент передбачає можливість їхнього скасування.

Для забезпечення відповідності вимогам Регламенту можуть вводитися спеціальні положення договору, які потребують попереднього схвалення наглядовим органом, а тому є потенційно менш привабливою опцією для оператора.

Кодекси поведінки й системи сертифікації. У ст. 49 Регламенту зазначаються два нових запобіжники – кодекси поведінки й системи сертифікації – які застосовуються як для оператора, так і для процесора.

Кодекси поведінки нагадують програми саморегуляції, які застосовуються в інших сферах, як засіб підтвердження наглядовим органам і споживачам факту дотримання компанією певних стандартів конфіденційності інформації. Згідно з положеннями Регламенту, такі кодекси можуть розроблятися спілками або іншими організаціями, які представляють операторів або процесорів, зокрема з метою транскордонної передачі даних. Дотримання цих кодексів у діяльності оператором або процесором, які займаються передачею персональних даних за межі ЄС, допоможе оператору підтвердити застосування належних запобіжників. Проекти кодексів діяльності мають подаватися на затвердження наглядовим органам згідно з положеннями ст. 38. Відповідно до ст. 41, нагляд за дотриманням кодексу поведінки може здійснювати акредитований і компетентний орган [7].

Як засіб підтвердження дотримання оператором або процесором певних стандартів, може розроблятися сертифікація захисту даних, знаки й позначки на рівні Євросоюзу. Як і кодекси поведінки, сертифікація доступна для операторів або процесорів за межами ЄС за умови підтвердження ними за допомогою договірних або інших юридично зобов'язальних документів їхньої готовності до застосування запобіжників, обов'язкових для захисту даних. Як додатково роз'яснюється ст. 42 і 43, системи сертифікації, знаки й позначки потребують подальших заходів із боку Європейської ради з питань захисту даних, яка може розробити загальноєвропейський знак захисту даних і яка буде відповідальною за оприлюднення інформації про сертифіковані організації в єдиній і загальнодоступній базі [8].

Юридично зобов'язальні корпоративні правила (ЮЗКП). Регламент, на відміну від Директиви, у ст. 46 прямо визнає ЮЗКП належним запобіжником і в ст. 47 наводить детальні умови для передачі даних на підставі ЮЗКП. Ці положення встановлюють необхідність схвалення ЮЗКП наглядовим органом відповідно до механізму узгодженості, згідно з положеннями ст. 63,

а також мінімальні вимоги до змісту ЮЗКП, такі як структура й деталі договору для зацікавленої групи, інформація про дані, спосіб врахування правилами загальних принципів захисту даних, процедури з дотриманням встановлених вимог і механізми дотримання вимог.

Винятки для окремих випадків. Ст. 49 визначаються винятки із заборони Регламенту на передачу персональних даних за межі ЄС без вживання належних захисних заходів. Ці винятки повторюють ті, що передбачені Директивою, до яких додається ще один, що передбачає визнання передачі даних «із поважних причин у законних інтересах оператора». Винятки застосовуються, коли:

– Суб'єкт даних прямо надав згоду на запропоновану передачу даних після отримання роз'яснень щодо ймовірних ризиків такої передачі для нього через відсутність визнання рівня захисту належним і застосування належних запобіжників.

– Передача є необхідною для виконання договору між суб'єктом даних і оператором або впровадження переддоговірних заходів на прохання суб'єкта даних.

– Передача є необхідною для укладення або виконання договору, укладеного в інтересах суб'єкта даних між оператором та іншою фізичною особою.

– Передача є необхідною з поважних причин та у суспільних інтересах.

– Передача є необхідною для обґрунтування, пред'явлення претензій юридичного характеру або відповіді на них.

– Передача є передачею даних із реєстру, який, відповідно до законодавства ЄС або держави-члена, існує для надання інформації громадськості, і дані якого є загальнодоступними або доступними будь-якій особі, здатній довести законність свого інтересу, лише в межах умов, встановлених законодавством ЄС або держави-члена для надання такого доступу в конкретному випадку.

Останній виняток дає більшу гнучкість, але також відповідає Регламенту, який вимагає наявності докладної й послідовної внутрішньоорганізаційної документації. Він передбачає, що, коли необхідність передачі даних неможливо обґрунтувати положеннями типового договору, ЮЗКП або будь-якими іншими винятками, передача до третьої держави або міжнародної організації може відбутися лише за умови, що вона «не є багаторазовою, стосується лише обмеженого кола суб'єктів даних, є необхідною з поважних причин у законних інтересах оператора, над якими не переважають інтереси або права і свободи суб'єкта даних, за умови, що оператор врахував усі обставини передачі даних, на підставі чого застосував для забезпечення захисту персональних даних належні запобіжники».

Такі формулювання є вразливими для тлумачення в широких межах як оператором даних, так і регуляторними органами, що спонукає службовців, відповідальних за захист даних, і наглядові органи до співпраці в розробці методичних рекомендацій, якими оператори зможуть керуватися в процесі діловодства та прийняття рішень.

Примітка. Згідно з положеннями ст. 13, під час отримання інформації про суб'єктів даних оператор зобов'язаний надавати суб'єктам даних певну інформацію. До неї прямо належить інформація про: а) намір оператора передати персональні дані до третьої держави або міжнародній організації; б) обґрунтованість такої передачі визнанням належності рівня захисту Єврокомісією; в) про належні або доречні запобіжники й способи їхнього отримання суб'єктом даних [9]. Така інформація має надаватися у стислій, прозорій, зрозумілій і легкодоступній формі, будучи викладеною ясною й простою мовою, і відповідати вимогам ст. 12 [10].

Штрафні санкції. Напевно, однією з найсуттєвіших відмінностей Регламенту від Директиви є запровадження значних штрафних санкцій за порушення його вимог щодо транскордонної передачі даних.

Порушення вимог до передачі даних, встановлених ст. 44–49, караються накладенням більшою з двох видів штрафних санкцій, передбачених Регламентом. Наслідком таких порушень може стати накладення «адміністративних штрафів у розмірі до 20 млн євро або, у випадку підприємства, до 4% загального світового обороту за попередній рік, залежно від більшого з них». Обставинами, які враховуються у накладенні штрафу, є «характер, тяжкість і тривалість порушення, його зумисний характер, заходи, вжиті для зменшення завданої шкоди, міра провини або історія порушень, спосіб, у який про факт порушення стало відомо наглядовому органу, виконання вимог, висунутих оператору або процесору, дотримання кодексу поведінки та інші обтяжувальні або пом'якшувальні обставини» [11].

Право на правовий захист. У разі незадоволення суб'єкта даних якістю реагування наглядового органу на його скаргу, він має право адресувати скаргу до національного суду.

Важливим прикладом застосування цього принципу є рішення Суду ЄС у справі Шремса (справа С-362/14), у якій суб'єкт даних був незадоволений якістю реагування ірландським наглядовим органом на його первинну скаргу. Він адресував свою скаргу до ірландського суду, який передав її на розгляд Суду ЄС, рішенням якого вимоги скаржника зрештою було задоволено [12].

Передача даних за межі Європейської економічної зони (ЄЕЗ). В аспекті передавання даних за межі ЄЕЗ Регламент повторює принципи й механізми, визначені Директивою щодо захисту даних, дещо розширюючи межі їхнього застосування.

Така передача може здійснюватися лише за умови виконання оператором та / або процесором умов, встановлених Регламентом, метою яких є забезпечення надійності гарантій належного рівня захисту, які надаються суб'єктам даних, під час передачі їхніх персональних даних до третьої держави.

Наслідком порушення вимог щодо передачі даних може стати накладення максимальних штрафних санкцій, передбачених Регламентом.

Передача персональних даних допускаються за таких обставин:

1. *Передавання до належної юрисдикції:* до третьої держави, окремої території, визначеної зони або міжнародної організації, які за визнанням Єврокомісії забезпечують належний рівень захисту даних. Існуючий перелік юрисдикцій, схвалених згідно з вимогами Директиви щодо захисту даних (напр., Швейцарія й Нова Зеландія) залишається чинним, і за Регламентом підлягає періодичному перегляду. Внаслідок останнього рішення Судової палати Європейського Союзу, програма сертифікації ЄС-США «Safe Harbor» («Безпечна гавань») втратила чинність для трансатлантичної передачі даних. Замість цього між ЄС та США було укладено угоду «Privacy Shield» («Про захист конфіденційності»), яка набула чинності 21 липня 2016 р., визначаючи механізм передавання даних з ЄС до США.

2. *Передача даних з ЄС до США згідно з положеннями угоди «Про захист конфіденційності »(Privacy Shield)*: у цій угоді Єврокомісія визнає належним рівень захисту, що забезпечують для персональних даних США. З 01 серпня 2016 р. підприємства США можуть у приватному порядку оформлювати сертифікацію відповідності принципам угоди «Про захист конфіденційності» в Міністерстві торгівлі США. До цих принципів належать: покладання обов'язків на компанії із США, які мають справу із персональними даними, накладення санкцій за порушення й встановлення жорсткіших умов для подальшої передачі персональних даних третім особам. США також надали гарантії чітких обмежень на доступ органів державної влади до персональних даних із метою боротьби зі злочинністю та захисту національної безпеки, впровадження запобіжників і механізмів нагляду. Передача персональних даних із ЄС до підприємства на території США, які взяли на себе зобов'язання виконувати угоду «Про захист конфіденційності», вважатиметься узгодженим із принципами цієї угоди, а тому відповідає стандартам захисту, які вимагаються законодавством ЄС [13].

Висновки. Регламент ЄС 2016/679 встановлює комплексний підхід до організації захисту персональних даних у разі їх транскордонної передачі. Положення Регламенту передбачають ефективні нормативно-правові і технічні механізми для безпеки даних під час їх передачі за межі ЄС. Регламент не лише полегшує транскордонну передачу даних за допомогою вдосконалених механізмів, але й передбачає процедури, умови та обмеження для передачі персональних даних до третіх країн або до міжнародних організацій. Важливим моментом виступає запровадження значних штрафних санкцій за порушення вимог Регламенту щодо транскордонної передачі даних. Що стосується передачі даних із ЄС до США, то тут ключовим моментом залишається питання подальшої практичної реалізації угоди «Про захист конфіденційності» («Privacy Shield»).

Список використаних джерел:

1. Стаття 42 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

2. Стаття 45 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

3. Стаття 46 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

4. Стаття 47 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

5. Стаття 48 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

6. Стаття 49 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

7. Стаття 42 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

8. Стаття 43 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

9. Стаття 13 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

10. Стаття 12 Регламенту (ЄС) 2016/679 про захист фізичних осіб у сфері опрацювання персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: http://eurlex.europa.eu/eli/reg/2016/679/oj.

11. URL: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/.

12. URL: https://www.whitecase.com/publications/article/chapter16remedies-and-sanctions-unlocking-eu-general-data-protection.

13. URL: https://www.ashurst.com/en/newsandinsights/legalupdates/general-data-protection-regulation/.