УДК 340.147
DOI https://doi.org/10.32782/2524-0374/2021-9/14

# АНАЛІЗ НОВИХ СТАНДАРТНИХ ДОГОВІРНИХ ПОЛОЖЕНЬ У КОНТЕКСТІ ПРАВИЛ БЕЗПЕЧНОЇ ГАВАНІ І РІШЕННЯ СУДУ ЄС «УПОВНОВАЖЕНИЙ ІЗ ЗАХИСТУ ДАНИХ ПРОТИ FACEBOOK IRELAND І МАКСИМІЛЛІАНА ШРЕМСА»

# ANALYSIS OF NEW STANDARD CONTRACTUAL PROVISIONS IN THE CONTEXT OF SAFE HARBOR RULES AND JUDGMENT OF THE EU COURT "COMMISSIONER FOR DATA PROTECTION AND PROCEEDINGS IN IRIS PROCEEDINGS"

**Іорданова О.Є., студентка IV курсу міжнародно-правового факультету**
*Національний юридичний університет імені Ярослава Мудрого*

**Лагутіна К.О., студентка IV курсу міжнародно-правового факультету**
*Національний юридичний університет імені Ярослава Мудрого*

Статтю присвячено дослідженню міжнародних договірних відносин, які зосереджені на регулюванні сфери обміну персональними даними, яке в межах країн Європейського Союзу регулюється спеціальним нормативним актом – Загальним регламентом Європейського Союзу про захист даних, натомість регулювання такої сфери в Україні здійснюється шляхом застосування Стандартних договірних застережень. Ключовим аспектом, який звертає увагу на важливість дослідження Стандартних договірних застережень, є те, що 4 червня 2021 року було затверджено нові Стандартні договірні застереження, які істотно змінюють регулювання сфери персональних даних як в Україні, так і в інших країнах світу, котрі не є членами ЄС. Аналізу піддаються питання, пов'язані із впливом рішення Суду Європейського Союзу «Уповноважений із захисту даних проти Facebook Ireland і Максиміллліана Шремса» на регулювання сфери передачі персональних даних. Звертається увага на специфічну термінологію приватних даних, яка міститься в Загальному регламенті Європейського Союзу про захист даних, зокрема, наводяться визначення таких понять, як «контролер», «оператор», «третя сторона», імпортер даних», «експортер даних», «одержувач», «треті країни» тощо. Зазначено також нормативно правові акти, які містять роз'яснення названих вище понять.

На основі аналізу рішення Суду Європейського Союзу «Уповноважений із захисту даних проти Facebook Ireland і Максиміллліана Шремса» та рішення Суду Європейського Союзу «Встановлений захист даних від Facebook Ірландія та Максиміллліана Шремса» було досліджено поняття «Щит конфіденційності» і встановлено, що такий щит представляє собою основу для регулювання трансатлантичного обміну даними в комерційних цілях. Окрім цього, було детально досліджено, на підставі яких критеріїв Суд Європейського Союзу визнав «Щит конфіденційності» недійсним.

Ретельну увагу приділено аналізу ключових змін, які були внесені під час прийняття нових Стандартних договірних застережень. Було підкреслено обґрунтовану необхідність внесення таких змін та ймовірні наслідки цього.

**Ключові слова:** персональні дані, щит конфіденційності, рішення Шремса, Стандартні договірні застереження, GDPR.

The article is devoted to the study of international contractual relations, which focus on regulating the exchange of personal data, which within the European Union is regulated by a special regulation – the General Regulation of the European Union on data protection, while regulating this area in Ukraine A key aspect that highlights the importance of studying the Standard Contractual Reservations is that on June 4, 2021, new Standard Contractual Reservations were approved, which significantly change the regulation of personal data both in Ukraine and in other non-member countries EU. Issues related to the impact of the decision of the Court of Justice of the European Union "Data Protection Commissioner against Facebook Ireland and Maximilian Schrems" on the regulation of personal data are analyzed. Attention is drawn to the specific terminology of private data contained in the General Regulation of the European Union on data protection, in particular, the definitions of such concepts as "controller", "operator", "third party", "data importer", "data exporter", "recipient are given", "third countries" etc. Normative legal acts are also mentioned, which contain explanations of the above concepts.

Based on the analysis of the decision of the Court of Justice of the European Union "Data Protection Commissioner against Facebook Ireland and Maximilian Schrems" and the decision of the Court of Justice of the European Union "Established data protection from Facebook Ireland and Maximilian Schrems" the concept of "Privacy Shield" that such a shield is the basis for regulating transatlantic data exchange for commercial purposes. In addition, it was examined in detail on the basis of which criteria the Court of Justice of the European Union declared the "Privacy Shield" invalid.

Careful attention has been paid to the analysis of key changes that have been made during the adoption of the new Standard Contractual Reservations. The legitimate need for such changes and the likely consequences of this were emphasized.

**Key words:** personal data, privacy shield, Schrems' decision, Standard contractual clauses, GDPR.

Зростання міжнародних договірних відносин протягом багатьох років стало результатом процесу глобалізації. Нині відбувається тісна взаємодія між країнами світу, обмін між такими країнами персональними даними, а це у свою чергу потребує гарантування достатнього рівня захисту персональних даних. Європейським Союзом (далі – ЄС) було здійснено ряд заходів у сфері персональних даних, для влучного розуміння яких варто розшифрувати специфічну термінологію. Під поняттям «контролера» (controller) розуміється сторона, яка самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних, водночас «оператор» (processor) – це особа, яка обробляє персональні дані від імені контролера. Ці дві особи призначають інспектора із захисту даних (Data Protection Officer), який забезпечує відповідність їхньої діяльності Загальному регламенту ЄС про захист даних. Під «третьою стороною» потрібно розуміти особу, яка не є суб'єктом даних або ж контролером, чи оператором, чи особою, яка під безпосереднім керівництвом контролера або оператора уповноважена опрацьовувати персональні дані. «Імпортером даних» визнається організація, розташована в межах третьої країни, яка отримує та обробляє персональні дані від експортера даних та від його імені. «Експортером даних» вважають контролера, який передає персональні дані. «Одержувачем» вважають особу, якій розкривають персональні дані незалежно від того, чи є така особа третьою стороною. Нормативні документи, які регулюють захист даних, також містять посилання на поняття «третіх країн». У рамках європейського законодавства прийнято вважати третіми кранами ті країни, які не ратифікували Загальний регламент ЄС про захист даних (далі – GDPR) [1].

Європейським Союзом у 2016 році було розроблено Загальний регламент ЄС GDPR, який діє як гарант захисту

персональних даних усіх осіб у межах ЄС та Європейської економічної зони (далі – ЄЕЗ).

Проте з цього випливає, що потрібно було знайти порозуміння між країнами Європейської економічної зони та третіми країнами, на яких не розповсюджується дія GDPR. Саме тому Європейським співтовариством було затверджено Стандартні договірні застереження (SCC), які є юридичним механізмом, що допомагає компаніям країн ЄЕЗ передавати персональні дані компаніям третіх країн, на яких не розповсюджується дія GDPR [2]. Відповідно до пункту 81 GDPR, договірні положення, що забезпечують відповідні гарантії захисту даних, можуть бути використані як підстава для передачі даних з ЄС у треті країни [1].

Стандартні договірні застереження (SCC) – це стандартні набори умов договору, на які підписуються як відправник, так і одержувач персональних даних [2]. Для влучного розуміння припустимо, що компанія збирає персональні дані суб'єкта даних та передає їх іншій компанії в країні, де GDPR не застосовується. У цьому випадку суб'єкт даних ризикує втратити захист GDPR щодо цих даних, включаючи здатність реалізовувати свої права суб'єкта даних. Завдяки SCC обидва суб'єкти господарювання передбачають передачу відповідно до юридично зобов'язуючої угоди, що містить пункти, які гарантують захист особистих даних одержувачем третьої країни.

4 червня 2021 року було затверджено нові Стандартні договірні застереження (SCC) [3]. Старі ж SCC було розроблено на основі Директиви ЄС 95/46/ЄС від 24 жовтня 1995 року про захист фізичних осіб під час обробки персональних даних та про вільне переміщення таких даних (далі – Директива ЄС 95/46/ЄС), яка вважається попередником GDPR [4]. Очевидною була застарілість як Директиви ЄС 95/46/ЄС, так і старих SCC у порівнянні із сучасними реаліями, що вимагало їх оновлення.

Старі SCC складалися з трьох рішень. Два рішення підлягали застосуванню під час передачі даних від контролерів ЄС контролерам, що не належать до ЄС. Є думка, що перше з трьох рішень – ЄК 2001/497/ЕС – вважається більш сприятливим для бізнесу завдяки своєму розвитку в співпраці з різними торговими асоціаціями [5]. Більш того, відповідно до відносин, регулювання яких підпадало під дію другого рішення, обидві сторони несуть солідарну відповідальність за зобов'язання щодо захисту даних [2]. Натомість третє рішення використовувалося для передачі даних від контролерів з ЄС до процесорів, що не входять до ЄС, це рішення також допускає можливість передачі субпідряднику робіт, якщо це забезпечувало належний рівень захисту прав і свобод суб'єктів даних [6]. Як ми можемо побачити, старі SCC регулювали відносини лише між контролерами, що ускладнювало процедуру взаємодії. У зв'язку з цим Європейською комісією вони на цей раз були викладені єдиним документом і містили ряд важливих відмінностей зі старими SCC.

Як вже було зазначено, 4 червня 2021 року Європейська комісія (далі – ЄК) прийняла оновлені Стандартні договірні положення для міжнародної передачі даних. До таких змін ЄК підштовхнуло рішення Суду Європейського Союзу Schrems II [7], яким було визнано недійсним Щит для захисту конфіденційності між ЄС та США. Основним призначенням Щиту для захисту конфіденційності між ЄС та США було надання американським компаніям можливості легше отримувати персональні дані від суб'єктів ЄС згідно із законодавством ЄС про захист конфіденційності.

Незважаючи на те, що в рішенні Schrems II Суд у кінцевому підсумку підтримав використання Стандартних договірних застережень (SCC) як законного механізму передачі даних відповідно до Загального регламенту ЄС про захист даних (GDPR), проте в рішенні також було зазначено, що закони країни перебування можуть підірвати захист у SCC, створюючи велику невизначеність та підвищений ризик щодо використання SCC для передачі даних між ЄС та США [7].

Вищезгадане судове рішення було винесено після визнання недійсним у 2015 році першого комплексу принципів передачі даних у США під назвою «Безпечна гавань» на основі заяви того ж самого Максиміліана Шремса [8]. Підстави для визнання недопустимого Щиту для захисту конфіденційності між ЄС та США суттєво схожі з підставами для визнання недопустимою «Безпечної гавані», і це рішення ще раз підкреслює складність узгодження європейських вимог щодо захисту даних з американською практикою захисту. Наведені рішення змінили законність передачі всіх даних у США, що здійснювалася винятково на основі програм Щиту для захисту конфіденційності між ЄС та США. Тож для передачі даних потрібні належні гарантії, і це все потребувало оновлення SCC уже з урахуванням «реалій сучасного бізнесу», при цьому забезпечуючи більшу гнучкість та захист для міжнародного обміну даними.

Звертаємо увагу на основні зміни нових Стандартних договірних положень (SCC).

По-перше, були прийняті деякі оновлення відповідно до GDPR, оскільки до цього Стандартні договірні положення значно відрізнялися від Загального регламенту про захист даних (далі – GDPR). GDPR вимагає, щоб міжнародні контракти на передачу даних містили певні положення щодо належного забезпечення захисту персональних даних ЄС. Оскільки старі SCC були зареєстровані до GDPR, вони не відповідали всім вимогам статті 28 (3) GDPR, що встановлює ключові положення, які повинен мати договір [2].

Було оновлено зобов'язання імпортера (організації, яка отримує персональні дані для обробки), ці зобов'язання почали включати посилення зобов'язань та прозорості (зокрема, щодо контролера перед контролером). Ставиться за вимогу використання чіткої та зрозумілої мови у відповідності до статті 12 GDPR. Окрім цього, доповнено деякі права суб'єктів даних, наприклад, право на доступ, стирання та права на заперечення проти обробки для прямого маркетингу тощо. Оновлені SCC упорядковують угоди про обробку даних, а саме дозволяють застосовувати єдину угоду між організаціями та постачальниками послуг ЄС і діловими партнерами, розташованими за межами ЄС [2].

Рішення Schrems II наголосило на необхідності додаткового захисту, зокрема для запобігання доступу третіх країн до персональних даних ЄС [7]. До цього здійснювалися додаткові заходи в разі, коли місцеве законодавство країни-імпортера даних надавало доступ державним органам до персональних даних ЄС та не дотримувалося Стандартних договірних положень. Оновлені SCC вирішують це питання двома положеннями. По-перше, організація, яка імпортує дані, повинна переконатись, що місцеве законодавство не буде перешкоджати її здатності дотримуватись SCC та надавати документацію щодо її аналізу [2]. По-друге, якщо уряд вимагає доступ до переданих персональних даних ЄС, імпортер даних повинен задовольнити такі вимоги шляхом апеляції, з додатковою вимогою повідомити експортера даних та навіть суб'єктів даних ЄС щодо таких державних запитів [2].

Незважаючи на те, що оновлені SCC у значній мірі впорядковують передачу даних, деякі вимоги виявляться обтяжливими. У світлі впливу рішення Schrems II організаціям доведеться залучати додаткову документацію щодо кожного виду передачі даних, щоб вони могли надати контролюючим органам документацію на запит. Оновлені SCC вимагають прикріпляти додатки, що вимагають більшої кількості деталей, ніж попередні SCC [2]. Тобто організації з метою передачі персональних даних ЄС повинні відкрито зазначати інформацію, що стосується збереження даних, пояснення щодо захисних заходів щодо конфіденційних даних, опису адміністративних та технічних гарантій, що стосуються імпорту даних тощо. Більше

того, оновлені SCC надають право громадянам ЄС подавати скарги на імпортерів [2]. Оскільки імпортери даних безпосередньо підпорядковуються наглядовим органам ЄС, то мешканці ЄС можуть подавати скарги проти імпортерів даних.

Друга особливість – це «одна точка входу», що охоплює широкий спектр сценаріїв передачі замість окремих наборів пунктів. Це означає, що існуватиме єдиний набір стандартних проекційних статей з деякими модулями, певними варіантами вибору [2]. Як наслідок, на експортера (організацію, що надсилає дані, як правило, це контролер даних) накладено суттєві зобов'язання, які націлені на перевірку здатності імпортера даних забезпечувати відповідність своєї діяльності оновленим положенням. Оскільки в реалізації немає конкретного посилання на будь-який контрольний список, експортер даних вирішує, як перевірити відповідність імпортера даних.

По-третє, оновлені SCC розроблені для охоплення багатьох сценаріїв та сторін, які можуть приєднатися до цих умов [2]. Це забезпечує більшу гнучкість для складних ланцюгів обробки за допомогою «модульного підходу» і пропонує можливість більше ніж двом сторонам приєднатися та використовувати однакові положення.

Тобто фактично було встановлено такі модулі для передачі даних: модуль 1 передбачає передачу даних від контролера до контролера, модуль 2 передбачає передачу даних від контролера до процесора, модуль 3 передбачає передачу даних від процесора до процесора, модуль 4 у свою чергу передбачає передачу даних від процесора до контролера [2].

Попередні SCC не передбачали передачу процесора до процесора або процесора до контролера, тому коли такі обставини виникали під час укладання контрактів, це призводило багатьох юристів до розгублення (юристи не могли дійти згоди або знайти рішення питання), а також до потенційного розриву в законній передачі даних. Крім того, оновлення вперше визнають, що експортер даних може бути суб'єктом, який не входить до ЄС, що корисно, коли, наприклад, експортер даних, що не входять до ЄС, підпадає під дію GDPR і хоче передати дані до іншого.

По-четверте, тепер оцінюванню буде підданий факт того, чи має третя країна закон, еквівалентний GDPR, або чи сумісною є практика, а також чи є законодавство проблематичним, що виражається в тому, що воно не має зазіхати на контрактні гарантії інструментів передачі фактично еквівалентного рівня захисту, тобто відповідати стандартам ЄС щодо основних прав та поважати суть основних прав і свобод, визнаних Хартією ЄС про основні права, або перевищувати необхідне та пропорційне в демократичному суспільстві втручання в такі права [2].

У разі якщо третя країна визнана такою, що має проблемне законодавство, експортер даних може призупинити передачу, здійснити додаткові заходи або продовжити передачу без здійснення додаткових заходів до тих пір, поки «проблемне законодавство» не застосовуватиметься на практиці до відповідної передачі даних або типів персональних даних. Оцінки передачі даних повинні бути чітко задокументовані в детальному звіті, щоб продемонструвати підзвітність.

Варто також зазначити, що для проведення такої оцінки будуть застосовані різні джерела інформації, але за умови, якщо вони є «релевантними, об'єктивними, надійними, перевіреними та загальнодоступними або доступними будь-яким іншим способом», які викладені в Додатку третьому до Рішення про виконання комісії (ЄС) 2021/915 від 4 червня 2021 року про стандартні договірні положення між контролерами та процесорами відповідно до статті 28 (7) Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради та статті 29 (7) Регламенту (ЄС) 2018/1725 Європейського Парламенту та ради, і включають можливість розгляду звітів від приватних постачальників даних, бізнес-аналітиків, від міжнародних організацій та внутрішні звіти імпортера даних про запити на доступ від державних органів [9].

Також нові SCC також застосовуються до субпроцесорів [2]. Наприклад, коли імпортер даних залучає субпроцесора відповідно до статті 28 (2) та (4) GDPR, SCC повинні розмежувати процедуру загального або спеціального дозволу від експортера даних та вимогу щодо письмового контракту із субпроцесором, що забезпечує той самий рівень захисту, що і в пунктах. Нові SCC, таким чином, діють відповідно до статті 28 GDPR, що регулює угоди про обробку даних (DPA), і до статті 46, що регулює транскордонні передачі, уникаючи необхідності укладання двох окремих угод.

Маємо також зазначити, що нові умови SCC також намагаються вирішити зобов'язання, пов'язані з рішенням Schrems II. Зокрема, існує практичний набір інструментів для виконання рішення Schrems II, тобто огляд різних кроків, які повинні зробити компанії, щоб виконати рішення Schrems II, а також приклади можливих «додаткових заходів», таких як шифрування, які можуть вживати компанії за необхідності.

Варто більш детально проаналізувати рішення Суду ЄС від 16.07.2020 р. по справі за № 311/18 «Встановлений захист даних від Facebook Ірландія та Максимілліана Шремса» [7].

16 липня Суд Європейського Союзу виніс своє довгоочікуване рішення у справі Комісії із захисту даних проти Facebook Ireland, Schrems. Це рішення анулює рішення Європейської Комісії щодо дозволу вільної передачі даних з ЄС до США, відповідно до Privacy Shield Framework, тобто так званий «Щит необхідності», який представляє собою основу для регулювання трансатлантичного обміну даними в комерційних цілях між Європейським Союзом та США і фактично наголошує на «неадекватності» США як сторони для передачі персональних даних, нівелюючи факт того, що США захищає персональні дані на належному рівні. Критерії адекватності були встановлені у виконавчому рішенні Комісії (ЄС) 2016/1250 від 12 липня 2016 року відповідно до Директиви 95/46/ЄС Європейського Парламенту та Ради про адекватність захисту, що надається ЄС–США [10].

Суд ЄС установив, що визначення Європейською комісією адекватності Щиту конфіденційності є недійсним із двох основних причин. По-перше, суд встановив, що програми нагляду США, які Комісія оцінила у своєму рішенні «Щит конфіденційності», не обмежуються необхідним та пропорційним, як того вимагає законодавство ЄС, а отже, не відповідають вимогам статті 52 Хартії ЄС про Основні права. Закони США мали кілька недоліків, які перешкоджають захисту персональних даних та порушують GDPR. По суті, Суд указав на далекосяжні можливості спостереження, які існують згідно із законами про національну безпеку США (а саме розділ 702 Закону про нагляд за зовнішньою розвідкою США (FISA), розпорядженням № 12333.

По-друге, суд визначив, що за все, що стосується нагляду в США, суб'єкти даних ЄС не мають судової компенсації та, отже, не мають права на ефективний засіб правового захисту в США, як того вимагає стаття 47 Хартії ЄС. Щит конфіденційності передбачав механізм захисту у формі омбудсмена. Проте роль не мала сили приймати рішення, які були б обов'язковими для розвідувальних служб США.

Частина 2.3. Наказу Президента США № 12333 дозволяє збір, зберігання та поширення у разі необхідності інформації, отриманої в ході законної зовнішньої розвідки, контррозвідки, міжнародного розслідування наркотиків або міжнародного тероризму, а також службово отриманої інформації, яка може вказувати на участь у діяльності, котра може порушувати федеральні, державні, місцеві чи іноземні закони [11].

У свою чергу стаття 702 Закону «Про невідповідність спостереженням у цілях зовнішньої розвідки» дозволяє Генеральному прокурору та директору Національної розвідки спільно проводити спостереження за особами, які знаходяться за межами США. Після отримання дозволу таке спостереження може тривати до одного року. Варто зазначити, що таке спостереження виражається в зборі, зберіганні та використанні даних про таку особу для стеження за нею в інтересах національної безпеки США [12].

Фактично стаття 702 санкціонує програми іноземного нагляду Агенцією національної безпеки (АНБ), такі як PRISM та деякі попередні заходи зі збору даних, які раніше були дозволені Програмою нагляду Президента з 2001 року.

Рішення Schrems II також кидає тінь на інші передачі персональних даних з Європи до США, враховуючи заяви СЄС про характер доступу уряду США до даних приватного сектору. Незважаючи на те, що рішення підтримує дію стандартних договірних положень, воно вимагає від компаній та регуляторних органів проводити аналіз у кожному конкретному випадку, щоб визначити, чи відповідають закордонні засоби захисту щодо доступу уряду до переданих даних стандартам ЄС.

Варто вказати на основні переваги рішення Schrems II. По-перше, воно наголосило на необхідності додаткового захисту, зокрема для запобігання доступу країн, що не входять до складу ЄС, до персональних даних громадян ЄС. Рішення підкреслює важливість захисту даних для світової комерції та вирішальну роль, яку відіграють фахівці в галузі конфіденційності у впровадженні захисту відповідно до закордонних вимог. Зокрема, тепер організація, яка імпортує дані, повинна переконатись, що місцеве законодавство не буде перешкоджати її здатності дотримуватися SCC та надавати документацію щодо її аналізу.

По-друге, якщо уряд вимагає доступ до переданих персональних даних ЄС, імпортер даних повинен задовольнити такі вимоги шляхом апеляції, з додатковою вимогою повідомити експортера даних та навіть суб'єктів даних ЄС щодо таких державних запитів.

Незважаючи на те, що оновлені SCC у значній мірі впорядковують передачу даних, деякі вимоги виявляться обтяжливими, і організації повинні розглянути відповідні заходи для забезпечення детальних та точних процесів перегляду. Наприклад, у світлі впливу Schrems II організаціям доведеться залучати додаткову документацію щодо кожного виду передачі даних, щоб вони могли надати контролюючим органам документацію на запит. Оновлені SCC включають додатки, що вимагають більшої кількості деталей, ніж попередні SCC. Організації повинні бути готові включати інформацію, що стосується збереження даних, пояснення захисних заходів щодо конфіденційних даних, описи адміністративних і технічних гарантій, що стосуються імпорту даних тощо для передачі персональних даних ЄС.

Більше того, оновлені SCC несуть більший ризик виконання для одержувачів даних. Тепер мешканці ЄС можуть подавати скарги на імпортерів даних, й імпортери даних будуть безпосередньо підпорядковуватися законодавству наглядових органів ЄС, хоча оновлені SCC забезпечують гнучкість для узгодження того, яким законодавством є держава-член ЄС. Зі збільшенням ризику застосування закону виникає необхідність ведення детальних записів як обґрунтування, так і відстеження передачі даних у випадку, якщо організація стає предметом всебічного перегляду.

Таким чином, SCCs було розроблено для відображення положень рішення суду у справі Schrems II шляхом надання договірним сторонам права здійснювати контроль над тим, чи можуть органи влади за межами ЄС отримувати доступ до персональних даних, які передаються з ЄС, і якщо так, то яким чином. Варто також зазначити, що нові стандартні договірні положення відображають нові вимоги Загального регламенту щодо захисту даних і відповідають реаліям, з якими стикаються сучасні суб'єкти підприємницької діяльності. Завдяки стандартизації та попередньому затвердженню SCC надають таким суб'єктам простий у реалізації шаблон, а тому такий крок у сфері захисту персональних даних є важливим, інноваційним та ефективним, а також таким, що дозволяє зробити передачу персональних даних у транскордонному аспекті безпечною.

**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) (2016), Official Journal of the European Union, no. 119. URL: https://eurlex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679 (дата звернення: 19.09.2021).

2. 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC. URL: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:EN:NOT

3. COMMISSION IMPLEMENTING DECISION (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915

4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

5. Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004D0915

6. Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council [2010] OJ L39/5. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&rid=4

7. Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems, C-311/18 (Court of Justice of the European Union, 16 July 2020). URL: https://curia.europa.eu/juris/liste.jsf?num=C-311/18

8. Judgment of the Court (Grand Chamber) of 6 October 2015 Maximillian Schrems v Data Protection Commissioner. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362

9. ANNEX III to the Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA relevance) "Technical and organisational measures including technical and organisational measures to ensure the security of the data. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0915

10. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

11. Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941. URL: https://www.archives.gov/federal-register/codification/executive-order/12333.html

12. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. URL: https://www.govtrack.us/congress/bills/110/hr6304/text#:~:text=The%20FISA%20Amendments%20Act%20of,Snowden%20in%202013%2C%20including%20PRISM