УДК 347+341.1
DOI https://doi.org/10.24144/2307-3322.2023.80.2.64

ШТРАФНІ САНКЦІЇ, ЯК ОСНОВНА ФОРМА ВІДПОВІДАЛЬНОСТІ ЗА ПОРУШЕННЯ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄС

Яворська І.М.,
кандидат юридичних наук,
доцент кафедри європейського права
Львівського національного університету
імені Івана Франка
ORCID: https://orcid.org/0000-0002-4504-9065
e-mail: iryna.iavorska@lnu.edu.ua

Стахура С.А.,
аспірант
факультету міжнародних відносин
Львівського національного університету
імені Івана Франка
e-mail: solomiya@gmail.com

Яворська І.М., Стахура С.А. Штрафні санкції, як основна форма відповідальності за порушення Загального Регламенту захисту персональних даних в ЄС.

У науковій статті досліджено правові засади стягнення штрафних санкцій за порушення норм Загального Регламенту захисту персональних даних. Обгрунтовано необхідність дослідження механізмів за допомогою яких реалізується процедура стягнення штрафів за порушення у сфері захисту персональних даних у межах Європейського Союзу. Проаналізовано норми Загального регламенту захисту персональних даних з метою використання досвіду держав-членів ЄС у сфері захисту персональних даних в контексті гармонізації законодавства України із правом ЄС.

У статті проаналізовано зміни у законодавстві щодо захисту персональних даних та встановлено найбільш часто застосовувані до поршників стягнення у вигляді штрафів, що накладались на компанії у таких країнах як Великобританія, Нідерланди, Іспанія. Формами відповідальності за порушення Регламенту є: адміністративний штраф, попередження, тимчасове припинення діяльності, або певних дій, що виконуються контролером чи оператором. Окрім даного переліку, держави-члени у своєму внутрішньому законодавстві мають право закріплювати додаткові форми відповідальності за порушення захисту персональних даних, якщо це не суперечить GDPR.

Також, визначено які саме порушення у сфері захисту персональних даних виступають підставами для накладення штрафів, а саме, встановлено, що це недотримання компаніями безпеки оброки персональних даних, неотримання умов та правил щодо надання згоди на обробку персональних даних, наступне використання компаніями персональних даних клієнтів після спливу строку, наданого для їх використання або ж передача даних клієнтів третім особам. Як зазначено прийняття Загального Регламенту захисту персональних даних посприяло забезпеченню стабільності законів, які регулюють питання, що стосуються конфіденційності персональних даних користувачів, а також відповідальності за порушення прав, що стосуються таких даних. Згідно Регламенту, будь-яка інформація, за якою можна ідентифікувати особу – це персональні дані.

Досліджено застосування механізмів накладення штрафних санкцій та проаналізовано обставини, що визначають розмір відповідальності за порушення у сфері захисту персональних даних.

Ключові слова: захист персональних даних, контролер персональних даних, оператор персональних даних, опрацювання персональних даних, наглядовий орган, стягнення адміністративного штрафу.

Iavorska I., Stahura S. Penalties as the main form of liability for violation of the General Regulation on Personal Data Protection in the EU.

The article outlines the legal basis of the penalties for violation of the General Data Protection Regulation in the EU. The necessity of studying the mechanisms by which the procedure for collecting fines for violations in the field of personal data protection within the European Union is carried out. Provisions of the General Data Protection Regulation are analyzed in order to apply the experience of EU member states in the field of personal data protection as well as in the context of harmonization of Ukrainian legislation with EU law.

The article analyzes changes in the legislation on the protection of personal data and identifies the most frequently applied penalties in the form of fines imposed on companies in countries such as Great Britain, Netherlands, and Spain. Forms of liability for violations of the Regulation are: administrative fine, warning, temporary suspension of activity, or certain actions performed by the controller or operator. In addition to the list, member states in their domestic legislation have the right to establish additional forms of liability for violations of personal data protection, if such a penalty does not contradict the GDPR.

In the article, it has also been determined which violations in the field of personal data protection act as grounds for imposing fines, namely, it has been established that these are non-compliance by companies with the security of personal data, non-observance of conditions and rules regarding consent to the processing of personal data, and the subsequent use by companies of personal data of customers after the leak the period provided for their use or the transfer of customer data to third parties. As mentioned above, the adoption of the General Data Protection Regulation contributed to ensuring the stability of normative acts that regulate issues related to the confidentiality of personal data of users, as well as responsibility for the violation of rights related to such data. According to the Regulation, any information by which a person can be identified should be interpreted as personal data. The article examines the application of mechanisms for imposing fines and analyzes the circumstances that determine the extent of liability for violations in the field of personal data protection.

Key words: personal data protection, data controller, data processor, data operator, personal data processing, supervisory body, administrative fee.

Постановка проблеми. Дослідження механізмів накладення адміністративних санкцій в рамках ЄС за порушення норм GDPR на даному етапі є надзвичайно актуальним. В умовах активізації онлайн сервісів в усіх сферах життя, починаючи від медицини, завершуючи наукою - кількість компаній, які підпадають під дію GDPR збільшується та, як наслідок актуалізується питання про те, як правильно збирати, обробляти та використовувати персональні дані для того, щоб уникнути ситуацій, які тягнуть за собою накладення штрафів, чи інших форм відповідальності.

Стан опрацювання. Питання видів і форм відповідальності, найчастіше застосовуваних санкцій за порушення законодавства у сфері захисту персональних даних виступали предметом дослідження у працях Тейлора Г., Мервінського О., Брижко В., Дяковського О., Кортукової Т. та інших дослідників.

Метою статті є аналіз практики застосування штрафних санкцій за порушення норм права ЄС у сфері захисту персональних даних.

Основний виклад матеріалу. Загальний регламент захисту персональних даних GDPR – "General Data Protection Agreement" набув чинності 25 травня 2018 року та розпочав новий етап розвитку права у сфері захисту персональних даних не лише на території Європейського Союзу, але й поза його межами, оскільки у статті 3 Регламенту закріплено, що дія його норм є екстериторіальною. [1] GDPR замінив Директиву про захист персональних даних 95/46/ЕС, що діяла на території ЄС із 24 жовтня 1995 року та значно змінив положення, що стосуються питань притягнення до відповідальності за порушення законодавства у сфері захисту персональних даних. Регламент закріпив у своїх положеннях значні розміри штрафів і надав право національним регуляторам на їхнє стягнення (Розд.6 GDPR).

Так, з початку дії регламенту контролюючими органами держав-членів ЄС було стягнено більш, ніж 80 тис. адміністративних штрафів. Згідно даних веб-порталу та кібербезпеки *Precise Security*, розмір сум штрафних санкцій за десять найбільших порушень вимог GDPR сягнув 746 мільйонів євро, а країнами-лідерами порушників GDPR за кількістю зафіксованих порушень GDPR є Великобританія, Нідерланди та Іспанія. [2] Найбільший штраф за період дії GDPR було накладено

на компанію *Amazon* у розмірі 746 мільйонів євро Національною комісією захисту персональних даних Люксембургу CNPD (Commission Nationale pour la Protection des Données). Справа була порушена внаслідок колективної скарги поданої у 2018 році французькою групою захисту конфіденційності *La Quadrature du Net* від імені 10 тис осіб. Ця група заявляла, що "система реклами, введена Amazon", застосовувалася "без їхньої чітко вираженої вільної згоди".

Наступна гучна справа пов'язана із діяльністю всесвітньо відомої компанії "Google". Штраф у розмірі 55 мільйонів доларів було накладено французьким контролюючим органом CNIL (Commission Nationale de l'Informatique et des Libertés) за недостатньо чітке формулювання своєї політики щодо отримання згоди на обробку даних та за ненадання своїм користувачам достатнього контролю над їхніми персональними даними.

Проаналізувавши справи про притягнення компаній до відповідальності за порушення у сфері захисту персональних даних, в контексті застосування GDPR, варто зазначити, що основними порушеннями, що стали підставами накладення штрафів є недотримання компаніями безпеки обробки персональних даних, недотримання умов надання згоди на отримання та обробку персональних даних, недостатність закріплених гарантій врегулювання, а також використання персональної інформації у маркетингових цілях. При цьому сума штрафів не є сталою, а нараховується кожному порушнику із врахуванням: характеру, важкості та тривалості порушення, умислу щодо вчиненої дії, котегорії даних, що постраждали внаслідок порушення, кількість постраждалих суб'єктів. [3]

Суб'єктам права захисту персональних даних важливо знати свої права, обов'язки та питання відповідальності, які виникають у них в контексті дії GDPR.

Захист персональних даних є однією із ключових цілей Європейського Союзу у сфері захисту прав людини, адже ще у Європейській конвенції про захист прав людини із основоположних свобод було закріплено: "Кожен має право на повагу до свого приватного та сімейного життя, до свого житла і кореспонденції" (ст.8)[1].

Основними учасниками процесу обробки та захисту даних згідно GDPR є:

– суб'єкт даних – це особа, яка може бути ідентифікована відповідно до GDPR;

– контролер – це фізична/юридична особа, або орган державної влади, основним завданням якого є визначення мети, завдань та засобів опрацювання персональних даних; - оператор – фізична/юридична особа, або орган державної влади, що здійснює опрацювання даних від імені контролера. По відношенню до юридичної особи це може бути, наприклад, компанія, яка діє в інтересах контролера, але є тим не менш незалежною юридичною особою. Особа, яка обробляє персональні дані зобов'язана дотримуватись у своїх діях вимог контролера. Наглядовий орган щодо захисту персональних даних – це незалежний державний орган, що засновується на території держави-члена ЄС. [2]

Таким чином, кожна держава-член ЄС зобов'язується створити на своїй території орган, що відповідатиме за захист персональних даних. Кількість наглядових органів у державі не обмежується одним, до прикладу можна взяти Федеративну Республіку Німеччину, яка складається із 16 федеративних земель, кожна з яких на своїй території має окремий наглядовий орган. [4]

Слід підкреслити, що представник кожного наглядового органу є членом Європейської Ради із захисту персональних даних. Такими органами у державах членах є: CNIL (Commission Nationale de l'Informatique et des Libertés) – Франція; DSB (Datenschutzbehörde) – Австрія, CNPD (Comissão Nacional de Protecção de Dados) – Португалія та ін.

Згідно Регламенту, суб'єкт чиї права, закріплені у нормах GDPR, були порушені, наділений правом подати скаргу до контролюючого органу в державі-члені ЄС за місцем проживання, місцем роботи, чи місцем порушення. У контексті GDPR відповідальними за його порушення є контролер та оператор. Будь-який контролер, залучений до опрацювання, несе відповідальність за шкоду, заподіяну опрацюванням, що порушує положення Регламенту. Оператор несе відповідальність за шкоду, заподіяну опрацюванням лише тоді, коли він не дотримується обов'язків за Регламентом, спрямовані безпосередньо на оператора, або якщо він діє поза чи всупереч законним вказівкам контролера. [4]

Основними формами відповідальності за порушення Регламенту є: адміністративний штраф, попередження, тимчасове припинення діяльності, або певних дій, що виконуються контролером чи оператором. Окрім даного переліку, держави-члени у своєму внутрішньому законодавстві мають право закріплювати додаткові форми відповідальності за порушення захисту персо-

нальних даних, якщо це не суперечить GDPR.[2] Так, до прикладу, у правових системах Данії та Естонії поняття адміністративного штрафу не передбачено. У Данії – штраф вважається кримінальною відповідальністю, а в Естонії штраф є покаранням за незначні правопорушення. Тому компетентні судові органи держав повинні враховувати рекомендації наглядових органів, щоб у будь-якому випадку покарання за порушення норм GDPR були дієвими, пропорційними та стримувальними. [1]

Штрафні санкції є найпоширенішою формою відповідальності за порушення GDPR, що передбачає грошове стягнення, яке накладається на відповідальну сторону. Найпоширенішими підставами для накладення такої форми відповідальності, як адміністративний штраф є: порушення, що стосуються категорії "чутливих даних"; порушення, внаслідок яких постраждала велика кількість осіб. [5]

У випадках вчинення незначних порушень, або порушень, які були усунуті і не нанесли шкоди застосовуються інші форми відповідальності, такі як попередження.

Порядок накладення адміністративного штрафу та його розмір визначені статтею 83 GDPR "Загальні умови для накладання адміністративних штрафів" передбачають: за незначні порушення GDPR розмір матеріальної відповідальності може сягнути 10 мільйонів євро, або 2% від річного обігу компанії за попередній фінансовий рік, залежно від того, яка сума буде більшою. за значні порушення, пов'язані з недотриманням основних принципів захисту персональних даних, розмір матеріальної відповідальності може сягнути 20 мільйонів євро, або 4% від річного обігу компанії за попередній фінансовий рік, залежно від того, яка сума буде більшою. [1]

При накладенні штрафу у кожному конкретному випадку враховуються наступні чинники: характер, тривалість та тяжкість порушення, враховуючи обсяг та мету обробки персональних даних; умисел винної особи, або ж вчинення порушення з необережності; ступінь співпраці із наглядовими органами з метою усунення, чи зменшення порушення; категорії персональних даних, які постраждали при правопорушенні.

Окрім цього, кожній країні-члену ЄС надається право для адаптування свого внутрішнього законодавства до вимог GDPR, а разом із тим визначати розмір штрафу, закріпивши таку градацію відповідальності у своєму внутрішньому законодавстві.[6] Статтею 83 GDPR закріплено, що накладення штрафу має бути ефективним, дієвим і співрозмірним характеру порушення.

Так, до прикладу найменшим штрафом, який був накладений у ЄС із початку дії GDPR був зафіксований у Австрії і сягнув 4 тисячі євро. Штраф було стягнено наглядовим органом Австрії – DSB за несанкціоноване відеоспостереження, що порушило приватність осіб у публічному місці. Разом з тим найбільшими штрафами, що сягають мільйонів євро пов'язані із використанням даних тисячі користувачів. Серед найбільших гучних справ є стягнення британським наглядовим органом – Офісом Інформаційної Безпеки Великобританії (ICO) сотні мільйонів доларів із таких компаній, як Facebook та British Airways. У 2019 році штраф із компанії Facebook було стягнуто у розмірі 644 мільйони євро, за конфлікт із компанією Cambidge Analytica. Тоді компанія зібрала дані про користувачів соцмережі для того, щоб вплинути на результат президентських виборів у США.

Наступна справа із початку дії Загального регламенту захисту персональних даних стосується міжнародної роздрібної компанії "H&M". Сума штрафу сягнула 35 мільйонів євро. Справа була заведена німецьким наглядовим органом та звинуватила компанію у тому, що вони зберігали заборонені Регламентом дані своїх працівників, що стосуються медичних даних, стану здоров'я і навіть детальну інформацію про їхнє приватне життя.. Важливу роль у даній справі відіграв Німецький Федеральний закон про конфіденційність даних Bundesdatenschutzgesetz, який вважається суворішим у аспектах питань, що відповідальності за порушення прав персональних даних. [4]

Висновки. Таким чином, проаналізувавши справи, в результаті яких було накладено штрафні санкції, можна прийти до висновку, що найбільш поширеними причинами правопорушень, що тягнуть за собою накладення штрафів є: недоліки безпеки: компанії не дотримуються усіх технічних та організаційних засобів, що можуть захистити персональні дані (наприклад, справа щодо British Airways); недотримання умов отримання згоди на обробку даних: часто компанії не створюють належну функцію та умови для коректного підтвердження особою надання даних (наприклад, справа щодо Google у Франції); використання даних у цілях маркетингу: такі випадки часто виникають, коли компанії використовують дані для маркетингових розсилок (електронна пошта, номер телефону та ін.) [2]

На основі вищевикладеного ми можемо відзначити, що надзвичайно важливим суб'єктом захисту персональних даних виступає наглядовий орган у державах членах. Так, згідно GDPR наглядові органи держав-членів наділено повноваженнями щодо надсилання попереджень контролерам, винесення догани, накладання обмежень. У контексті накладення штрафних санкцій, наглядові органи мають повноваження щодо їх накладення відповідно до статті 83 GDPR.

Важливо відмітити, що накладення штрафних санкцій стосується не лише контролерів та операторів, що зареєстровані на території ЄС, але й тих хто знаходиться поза його межами, адже я зазначалось вище у статті – GDPR має екстериторіальну дію. [3] Як приклад можна навести справу, що стосувалась канадської компанії AggregatelIQ, яка займається цифровим маркетингом та розробкою програмного забезпечення через її зв'язок із компанією Cambridge Analytica. Зокрема, у 2016 р. AggregatelIQ використала персональні дані з Facebook, якими раніше заволоділа Cambridge Analytica, для розробки програмного забезпечення, за допомогою якого здійснювалася цільова реклама виборців у США під час президентської компанії. Контролюючий орган Великобританії (ICO) застосував штраф у розмірі 17 мільйонів фунтів стерлінгів.

В Україні поки відсутні численні прецеденти щодо застосування відповідальності за порушення захисту персональних даних згідно до GDPR, проте як бачимо із світової практики, такий прецент може відбутись і у найближчий час, особливо в сучасних тенденціях використання даних та інформаційних ресурсів. На український бізнес дія Регламенту може поширюватись у випадках: присутності представництва у будь-якій формі на території ЄС; моніторингу поведінки суб'єкта даних на території ЄС; просування товарів та послуг європейцям у межах ЄС.

Отже, якщо діяльність компанії підпадає під один із вищезазначених пунктів, необхідно забезпечити організаційні та технічні заходи, що передбачаються Регламентом.

Таким чином, як зазначалося, штрафні санкції займають центральне місце серед усіх форм відповідальності за порушення захисту персональних даних у ЄС, адже саме вони є тим важелем, який на думку авторів GDPR повинен забезпечувати належний захист персональних даних як в ЄС, так і поза його межами, адже дія Регламенту є екстериторіальною. GDPR, у порівнянні із іншими документами у сфері захисту персональних даних, що діяли до нього значно збільшив розміри штрафів та надав повноваження державам-членам для адаптації розмірів штрафів у їхнє внутрішнє законодавство. Так, загальні умови для накладання адміністративних штрафів закріплені у 83 статті Регламенту.

Основними учасниками процесу обробки персональних даних є: суб'єкт даних, контролер, оператор, наглядовий орган. Пункт 1 статті 82 Регламенту встановлює, що будь-яка особа, яка зазнала матеріальної чи нематеріальної шкоди в результаті порушення положень Регламенту, має право на отримання компенсації від контролера чи процесора за завдану шкоду. Як ми бачимо, відповідальними за порушення норм GDPR виступають контролер, який визначає основну мету та цілі збору, обробки та використання персональних даних та оператор, який здійснює свої функції відповідно до поставлених йому завдань контролером. Суб'єктом, що наділений функціями щодо притягнення до відповідальності, контролю та стягнення адміністративних штрафів є наглядовий орган, який створюється та діє на території кожної держави-члена ЄС. Функкції наглядового органу перелічені у статті 58 Регламенту.

Розмір штрафу, який накладається наглядовим органом на порушника не є однаковим та сталим для всіх, він розраховується у кожному конкретному випадку із врахуванням таких чинників, як: характер, тяжкість, кількість постраждалих, мета обробки, навмисність чи ненавмисність скоєного правопорушення, категорії персональних даних, які постраждали внаслідок порушення, ступінь співпраці з наглядовими органами з боку контролера та процесора. За незначні порушення розмір штрафу може сягнути максимально 10 мільйонів євро, або 2% від річного обороту компанії за попередній фінансовий рік, в залежності від того, яка сума буде більшою. За значні порушення розмір штрафу може сягати максимум 20 мільйонів євро, або 4% від річного обігу компанії за попередній фінансовий рік, в залежності від того, яка сума буде більшою. Так, найменший штраф за 2 роки дії GDPR був зафіксований австрійським наглядовим органом DSB у розмірі 4 тисячі євро за неправомірну відеозйомку перехожих, а найбільшим штрафом, який уже стягнуто зафіксовано наглядовим органом Великобританії (ISO) у розмірі 55 мільйонів євро із всесвітньо відомої соціальної мережі Facebook за збір даних, який було згодом використану для впливу на вибори президента Америки. Окрім цього слід підкреслити, що штрафні санкції можуть бути накладені не лише на території ЄС прикладом цього є стягнення штрафу наглядовим органом

Великобританії із канадської компанії AggregatelIQ у розмірі 17 мільйонів фунтів стерлінгів за використання персональних даних із мережі Facebook .[6] Тому, ми можемо стверджувати, що штрафні санкції можуть у майбутньому стосуватись і України, оскільки все більше і більше компаній, особливо у сфері медицини, транспорту та IT співпрацюють із громадянами ЄС.

Норми GDPR будуть застосовуватись до українських компаній у випадках: компанія є оператором персональних даних або обробляє персональні дані та знаходиться на території ЄС; компанія розташована за межами ЄС, але обробляє персональні дані громадян ЄС. Це також стосується випадків, коли компанія займається продажом товарів або послуг та здійснює моніторинг поведінки користувачів, що перебувають на території ЄС.

Таким чином, аналізуючи практику застосування штрафних санкцій європейськими наглядовими органами за порушення GDPR, можна стверджувати, що штрафи, зовсім різні та значною мірою залежать від вчиненого правопорушення, завданих збитків і заходів, вжитих для мінімізації порушення. Штрафи, як правило, накладаються в тих випадках, коли порушення стосуються: великих обсягів персональних даних, внаслідок яких страждає велике коло осіб (як у випадку з Google); чутливих персональних даних (як у Португалії в ситуації з медичними даними пацієнтів).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 96/46/ЄС (Загальний регламент про захист даних) / Європейський Союз. . Цит. 24.11.2014 р. URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf.
2. Тищенко К. GDPR – нові виклики для обробників персональних даних. *Юридична газета online*. URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr--novi-vikliki-dlya-obrobnikiv-personalnih-danihvukrayini.html.
3. Духовна О. Вчимося на помилках: найбільші штрафи за порушення норм GDPR. *Юридична газета online.* URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/vchimosya-na-pomilkah-naybilshi-shtrafi-za-porushennya-norm-gdpr.html.
4. Колченогова О. GDPR для юристів, або я підготуватися до неминучих змін. *Юридична газета online.* URL: https://yur-gazeta.com/dumka-eksperta/gdpr-dlya-yuristiv-abo-yak-pidgotuvatisya-do-neminuchih-zmin-.html.
5. Бем М.В., Городинський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с. URL: http://er.ucu.edu.ua/bitstream/handle/1/449/Protection%20of%20personal%20data.pdf?sequence=1&isAllowed=y.
6. Волосецький В.О. Іноземний досвід правового регулювання захисту персональних даних. *Міжнародний науковий журнал*. URL: https://www.inter-nauka.com/uploads/public/14815322304340.pdf.
7. "Аналіз законодавства про захист персональних даних України" Звіт. / підгот. АС "Саєнко Харенко" / Міністерство Цифрової Трансформації України. URL: http://ecpl.com.ua/wp-content/uploads/2020/09/UKR_09142020_CEP_Finalnyy-zvit.pdf.
8. Мервінський О. «Чутливі» персональні дані. Як вони захищені? URL:http://yurincom.com/ua/legal_practice/analitychna_yurysprudentsiia/chutlyvi_personalni_dani__yak_vony_zakhyshcheni_-publication/.
9. Тейлор Г. Захист персональних даних в ЄС: настав час змін. URL: http://pravo.org.ua/politicreformand%20constitutionslaw/%20human.