Інформаційна довідка
щодо штрафних санкцій за порушення вимог GDPR*

Анотація. В Інформаційній довідці розглянуто досвід європейських держав стосовно застосування штрафних санкцій за порушення вимог Загального регламенту ЄС із захисту даних (GDPR), зокрема у контексті розмірів таких штрафів.

Ключові слова: *штраф, Регламент GDPR, персональні дані, захист даних, приватне життя, Європейський Союз.*

Вступ. У Європейському Союзі захист персональних даних осіб у межах Європейського Союзу та Європейської економічної зони врегульовано Загальним регламентом ЄС із захисту даних (GDPR, DSGVO)[1] (далі – Регламент GDPR або GDPR). Наявність цього документа не вимагає від національних парламентів прийняття законів, які уможливлюють його дію, він є *безпосередньо* зобов'язальним і застосовним.

При формуванні національних вимог щодо обробки персональних даних в європейських державах використовувалися два підходи:

(1) генеральний – полягав у прагненні створити єдиний і всеосяжний закон про захист сфери приватного життя і був пов'язаний зі спробами теоретичного обґрунтування «загального та абсолютного права на невтручання в приватне життя» (наприклад, окремі держави включили право на захист персональних даних до Конституції: Швеція, Бельгія, Греція, Нідерланди);

(2) секторальний (або галузевий) – запровадження спеціалізованих законів для захисту від певного виду (типу) посягань на сферу приватного життя, або для кожної галузі чи сектору людської діяльності, яка є потенційним джерелом загроз для права людини на невтручання у її приватне життя.

У більшості країн ЄС сучасні національні системи правового регулювання обробки та використання персональних даних застосовують так званий змішаний принцип, якому притаманні певні аспекти «генерального» і «галузевого» підходів.

Національне законодавство у сфері захисту даних, як правило, складається з: базового або системотворчого закону; комплексу галузевих законів, які забезпечують захист персональних даних у різних контекстах. Регулюючими компонентами сучасних систем захисту персональних даних є також національний уповноважений орган (або система органів) захисту даних та корпоративні засоби захисту (саморегулювання у формі кодексів поведінки/практики). Національний орган (або органи) із захисту даних, як

[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). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

правило, наділяється реєстраційно-дозвільними, контрольно-наглядовими, арбітражними, експертними та методологічними функціями. Хоча процедурні норми викладаються по-різному, відповідно до правової системи кожної держави, існує згода щодо цілей, які мають бути забезпечені цими нормами. Національні законодавства включають, як мінімум, такі принципи, зафіксовані в міжнародних документах: відкритість – суспільство має бути поінформовано про наявність баз персональних даних, які знаходяться у розпорядженні урядових органів, організацій та установ; можливість доступу суб'єкта даних до даних про себе та можливість коригувати неточні чи застарілі дані; збір персональних даних та обсяг цих даних має бути обмежений відповідно до цілей збору; обмеження використання – персональні дані повинні використовуватися тільки з метою, для яких вони збиралися; обмеження розкриття – персональні дані можуть бути розкриті лише з законною метою та за згодою суб'єкта даних; безпека – дані повинні бути захищені від втрати, несанкціонованого доступу, знищення, використання або модифікації[2].

Регламент (ЄС) 2016/679 (GDPR) запровадив узгоджену систему штрафів у всьому Європейському Союзі як засіб забезпечення дотримання правової бази захисту даних. Однак збільшення наглядових повноважень *не було рівномірним* у різних юрисдикціях. Наприклад, у Сполученому Королівстві Закон про захист даних 1998 року передбачав максимальний штраф за недотримання вимог у розмірі 500 000 фунтів стерлінгів, а в Іспанії – 600 000 євро, тоді як аналогічні регулятори в Польщі та Бельгії не мали таких повноважень штрафувати. Приблизно через п’ять років Європейська рада із захисту даних (EDPB) опублікувала нові вказівки щодо розрахунку відповідно до GDPR. Ці нові вказівки мають на меті забезпечити ясність і узгодженість у розрахунку штрафів у державах-членах ЄС і гармонізувати методологію, що використовується органами із захисту даних (DPA) для такого розрахунку.

Отже, з прийняттям GDPR перед державами-членами поставлено завдання забезпечити узгодженість його вимог із нормами національного законодавства, зокрема щодо уніфікації функціональних обов'язків контролерів та обробників персональної інформації; запровадження адекватних санкцій за допущені порушення законодавства про захист персональних даних та забезпечення ефективної співпраці між наглядовими органами держав-членів ЄС.

У той же час GDPR передбачає можливість державам-членам запроваджувати власні правила з великого кола питань, у тому числі щодо обробки особливих категорій персональних даних (sensitive data), а також

[2] Три сценарії міжнародного управління конфіденційністю даних: на шляху до міжнародної організації із захисту конфіденційності даних. URL: http://moritzlaw.osu.edu/students/groups/is

встановлювати обставини, за яких обробка особливих категорій персональних даних, незважаючи на надзвичайність ситуації та відсутність згоди суб'єкта, буде визнана правомірною.

Основна частина. Загальні умови для накладання адміністративних штрафів визначені статтею 83 Регламенту GDPR[3].

Кожний наглядовий орган повинен забезпечити, щоб накладення адміністративних штрафів у зв'язку з порушеннями цього Регламенту, вказаними в параграфах 4, 5 і 6, у кожному окремому випадку *було дієвим, пропорційним і стримувальним.*

Під час вирішення питання стосовно накладання адміністративного штрафу, а також щодо розміру адміністративного штрафу в кожному окремому випадку необхідно звертати належну увагу на таке:

(a) специфіку, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм;

(b) навмисний або недбалий характер порушення;

(c) будь-які дії, вжиті контролером або оператором для зниження рівня шкоди, заподіяної суб'єктами даних;

(d) ступінь відповідальності контролера або оператора, зважаючи на технічні та організаційні інструменти, які вони застосовують відповідно до статей 25 і 32;

(e) будь-які належні попередні порушення з боку контролера або оператора;

(f) рівень співпраці з наглядовим органом для відшкодування порушення і скорочення можливих негативних наслідків порушення;

(g) категорії персональних даних, на які вплинуло порушення;

(h) спосіб, у який наглядовому органу стало відомо про порушення, зокрема, або, і якщо так, то якою мірою, контролер або оператор повідомив про порушення;

(i) якщо заходи, вказані в статті 58(2), були раніше призначені проти відповідного контролера або оператора щодо того самого питання, - відповідність цим заходам;

(j) дотримання затверджених кодексів поведінки відповідно до статті 40 або затверджених кодексів поведінки відповідно до статті 42;

(k) будь-який інший обтяжувальний або пом'якшувальний фактор, застосовний до обставин справи, такий як отримана фінансова вигода або витрати, яких вдалося уникнути, прямо чи опосередковано, від порушення.

Якщо контролер або оператор навмисно чи за недбалістю, для тих самих чи пов'язаних операцій опрацювання, порушує декілька положень

[3] 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 (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

цього Регламенту, загальна сума адміністративного штрафу не повинна перевищувати суму, визначену для найтяжчого порушення.

За визначені порушення GDPR може бути накладено штраф:

(1) у розмірі ***до*** 10 млн євро або, у випадку підприємства, до 2% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою:

(a) обов'язки контролера і оператора відповідно до статей 8, 11, 25-39, 42, 43;

(b) обов'язки органу з сертифікації відповідно до статей 42 і 43;

(c) обов'язки органу з моніторингу відповідно до статті 41(4);

(2) у розмірі ***до*** 20 млн євро або, у випадку підприємства, до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою:

(a) основні принципи опрацювання, в тому числі умови надання згоди, відповідно до статей 5, 6, 7 і 9;

(b) права суб'єктів даних відповідно до статей 12-22;

(c) акти передавання персональних даних до одержувача в третій країні чи до міжнародної організації відповідно до статей 44-49;

(d) будь-які обов'язки відповідно до закону держави-члена, ухваленого згідно з главою IX;

(e) невідповідність постанові або тимчасовому чи остаточному обмеженню на опрацювання чи призупинення потоків даних наглядового органу відповідно до статті 58(2) або ненадання доступу як порушення статті 58(1).

Дотримання GDPR в європейських країнах відстежується через огляд штрафів і санкцій, накладених органами захисту даних у ЄС відповідно до Регламенту GDPR (*звіт GDPR).*

Дослідивши звіт GDPR Enforcement Tracker[4] у розрізі європейських держав можна констатувати, що ними імплементовано Регламент GDPR і, накладаючи штраф, контролюючий орган відповідної держави, здебільшого, посилається на статті цього Регламенту ЄС і досить рідко на національне законодавство, наприклад: в Італії – на Кодекс конфіденційності[5]; у Швеції – Закон про електронні комунікації[6] (Додаток 1).

Більшість країн мають спеціальні закони про захист даних, в яких визначені загальні засади щодо штрафних санкцій, які «перегукуються» з правилами Регламенту GDPR. Наприклад, із Закону ***Бельгії*** від 30 липня 2018 року про захист осіб у зв'язку з обробкою персональних даних («Бельгійський закон про захист даних[7]») випливає, що:

---

[4] URL: https://cms.law/en/int/publication/gdpr-enforcement-tracker-report

[5] ITALIAN PERSONAL DATA PROTECTION CODE. Legislative Decree no. 196 of 30 June 2003. URL: https://www.privacy.it/archivio/privacycode-en.html

[6] Swedish Lag (2003:389) om elektronisk kommunikation (i ändrad lydelse upp till Lag (2017:406)). URL: https://www.wipo.int/wipolex/en/legislation/details/17726

[7] Act on the protection of natural persons with regard to the processing of personal data. URL: https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf

– перший рівень становить до 10 мільйонів євро або 2% річного світового обороту за попередній рік, залежно від того, що вище (для порушень статті 11 (обробка, яка не потребує ідентифікації) та статей 25–39 (загальні зобов'язання обробників та контролери));

– другий рівень становить до 20 мільйонів євро або 4% від річного обороту попереднього року, залежно від того, що вище (може бути видано за порушення статей: 5 (принципи обробки даних); 6 (законність обробки); 7 (умови згоди); 9 (обробка особливих категорій даних).

Окрім того, в Бельгії передбачається покарання за порушення Закону про захист даних (а також самого GDPR), з максимальним адміністративним штрафом у 30 000 євро. Бельгійський закон про захист даних також роз'яснює, що контролер та/або обробник несуть цивільну відповідальність за сплату штрафів, які були накладені на його підрядника чи агента.

Перший національний стандарт, адаптований до положень GDPR, ухвалено у 2017 році Федеральною радою ***Німеччини***: Закон про адаптацію закону про захист даних до Регламенту (ЄС) 2016/679 та імплементацію Директиви (ЄС) 2016/680) (Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 i zur Umsetzung der Richtlinie (EU) 2016/680 o Bundesdatenschutzgesetz BDSG)[8].

Законом про захист даних (Bundesdatenschutzgesetz, BDSG[9]) деталізовано вимоги GDPR щодо призначення співробітника, відповідального за обробку персональних даних (DPO): в установі має бути призначений відповідальний співробітник, якщо понад 20 осіб здійснює автоматизовану обробку персональних даних або якщо обробка пов'язана з передачею та анонімізацією даних, дослідженні ринків, DPO мають бути надані наглядовому органу; прямо заборонено передавати пул (набір) персональних даних, отриманих без дозволу суб'єктів – у комерційних цілях або заподіяння шкоди суб'єктам; дозволено відеоспостереження у загальнодоступних місцях: державні органи мають право здійснювати з метою охорони життя та здоров'я громадян (для запобігання загрозам державній та громадській безпеці, кримінальних злочинів), якщо відеоспостереження необхідне для захисту законних інтересів та ці інтереси вищі, ніж право суб'єктів на охорону персональних даних осіб; дозволено обробку даних для скорингу перед укладенням договору, за умови: дотримання законодавства щодо застосування заходів захисту даних; розрахунок значення ймовірності відбувається на основі науково визнаної математико-статистичної процедури; адресні дані не використовувалися виключно для розрахунку значення ймовірності; у разі використання

[8] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 i zur Umsetzung der Richtlinie (EU) 2016/680 o Bundesdatenschutzgesetz BDSG.URL: https://dip.bundestag.de/vorgang/gesetz-zur-anpassung-des-datenschutzrechts-an-die-verordnung-eu-2016-679/79680

[9] Bundesdatenschutzgesetz (BDSG). URL: https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html#BJNR209710017BJNG002400000

адресних даних суб'єкта було поінформовано про передбачуване використання цих даних до розрахунку значення ймовірності. Вік надання згоди на обробку даних – 16 років.

При виявленні порушень правил захисту даних або інших недоліків в обробці персональних даних уповноважений орган (особа) має діяти відповідно до статті 58 Регламенту (ЄС) 2016/679 (§ 16 Закону про захист даних). Тобто фінансові санкції у виді дворівневих штрафів (до 10 млн і до 20 млн) накладаються за правилами Регламенту GDPR.

Водночас, за порушення вимог Закону про захист даних можуть бути застосовані й адміністративні штрафи у розмірі до 50 000 євро (§ 43 Закону про захист даних), а також притягнуто особу до кримінальної відповідальності з покаранням позбавлення волі на строк до трьох років або штрафом (§ 42 Закону про захист даних).

У ***Франції*** на додаток до GDPR діє оновлений Закон про обробку даних, файлів і свободи (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)[10], положення якого передбачають такі особливості: персональні дані померлих осіб можуть бути оброблені, якщо суб'єкт даних не висловив свою відмову за життя; вік надання згоди на обробку даних – 15 років; будь-який суб'єкт має право зареєструватися у спеціальному реєстрі – Bloctel (https://www.bloctel.gouv.fr) і тим самим висловити відмову від рекламних дзвінків та листів. Така відмова діє 3 роки і може продовжуватися на той самий термін. Водночас, якщо суб'єкт уклав договір з контролером – йому можна дзвонити, але пропонувати товари та послуги вже не можна, якщо його дані містяться в Bloctel; у відносинах працівник-роботодавець отримання письмової згоди на обробку персональних даних є необов’язковою за мовчазної згоди особи; дозволено відстеження геолокації транспортних засобів, керованих співробітниками, якщо це здійснюється під час роботи; дозволено запис телефонних розмов співробітників, якщо це відповідає заздалегідь визначеній меті, наприклад, для навчання або оцінки якості обслуговування; дозволено вивчення робочої електронної пошти, якщо листи не мають позначки «особисте».

Організація може бути піддана санкціям за недотримання GDPR у рамках скарги або перевірки, проведеної CNIL (Національна комісія з питань інформатики та свободи, Commission nationale de l'informatique et des libertés). За порушення правил GDPR застосовуються фінансові санкції у розмірах, визначених Регламентом (ЄС) 2016/679. Окрім того існує відповідальність за порушення правил закону про захист даних: позбавлення волі до 5 років;

[10] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

штраф для юридичних осіб до 300 000 євро (статті 20-23 Закону, із змінами 2024 року; розділ V Кримінального кодексу[11]).

На ***Кіпрі*** Законом про захист фізичних осіб від обробки персональних даних і вільного поширення таких даних (Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018, із змінами 2022 року)[12] передбачено певні особливості обробки персональних даних. А саме: генетичні та біометричні дані не можуть бути оброблені з метою отримання медичного страхування та страхування життя, навіть якщо суб'єкт даних дав згоду; зобов'язання отримати консультацію та схвалення наглядового органу під час передачі спеціальних категорій персональних даних у третіх осіб, які перебувають в інших державах; використання відеоспостереження на робочому місці та біометричних даних працівників можливе виключно, якщо роботодавець може довести необхідність проведення цих заходів або у тому випадку, коли для досягнення цілей контролю немає інших способів; використання cookie дозволено лише за згодою користувача, якому має бути надана чітка та вичерпна інформація про цілі обробки, за винятком випадків використання cookie, необхідних для надання послуг суб'єкту і без яких функціонування неможливе.

Має місце додаткова відповідальність (адміністративна/кримінальна) (до дворівневої фінансової відповідальності, встановленої Регламентом GDPR): позбавлення волі до 3 років та/або штраф у розмірі не більше 30 000 євро; позбавлення волі не більше 1 року та/або штраф не більше 10 000 євро; позбавлення волі до 5 років та/або штраф у розмірі не більше 50 000 євро; штраф, застосовуваний до державного органу, не може перевищувати 200 000 євро (Розділ X Закону). У разі несплати адміністративного штрафу, його сума стягується як цивільний борг перед Республікою (частина друга статті 32 Закону).

В ***Іспанії***, відповідно до Закону про захист персональних даних та гарантії цифрових прав (Ley Orgбnica 3/2018 de Protecciyn de Datos Personales y garantna de los derechos digitales)[13], контролеру надається можливість самостійно прийняти рішення по скарзі. У окремому розділі задекларовано гарантії цифрових прав, зокрема щодо захисту приватного життя у сфері праці, наприклад, про право на недоторканність приватного життя та право використання цифрових пристроїв на робочому місці, право на недоторканність приватного життя від використання пристроїв

[11] Code pénal. URL: https://www.cnil.fr/fr/les-sanctions-penales

[12] Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (N. 125(I)/2018). URL: http://www.cylaw.org/nomoi/enop/non-ind/2018_1_125/full.html

[13] Ley Orgбnica 3/2018 de Protecciyn de Datos Personales y garantna de los derechos digitales). URL: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

відеоспостереження та звукозапису на робочому місці та використання систем геолокації при виконанні трудових зобов'язань. Також передбачено: право на свободу вираження поглядів та інформації в Інтернеті; наявність алгоритмів у соціальних мережах (та публічних ресурсах), що дозволяють виправити та видалити опубліковану інформацію; право на забуття у пошукових системах та соціальних мережах, тощо.

Особливо детально врегульовано питання згоди на використання файлів cookie, яка може вважатися отриманою на законних підставах, якщо на сайті хоча б мінімум інформації про використання надається за допомогою банера. Згодою є однозначна дія суб'єкта, що засвідчує згоду – зокрема, використання смуги прокручування, перехід за посиланнями на відвідуваному сайті. Вік згоди на обробку персональних – 14 років.

Розмір штрафу за порушення Закону про захист даних залежать від тяжкості порушення (статті 72-74): за незначні порушення: до 40 000 євро; за серйозні порушення: від 40 001 євро до 300 000 євро; за дуже серйозні порушення: від 300 001 євро до 20 мільйонів євро або 4% від річного обороту (залежно від того, яка сума більша). У такому підході у визначенні розмірів відповідальності застосовано комбінацію штрафу за порушення GDPR і адміністративного/кримінального штрафу, передбаченого на національному рівні.

Сам порядок накладення адміністративних/кримінальних штрафів регламентується відповідним процесуальним законодавством. Як правило, порядок накладення штрафних санкцій носить адміністративний (не судовий) характер, з можливістю судового оскарження. Судове провадження щодо накладення штрафів застосовується в Бельгії.

В цілому, існує тенденція збільшення штрафних санкцій для юридичних осіб, як на практиці при – застосуванні положень GDPR, так і на законодавчому рівні – при застосуванні адміністративної/кримінальної відповідальності.

Водночас, розрахунки штрафів здійснюються за внутрішніми інструкціями, що базуються на європейських інструкціях Європейської ради із захисту даних (European Data Protection Board, EDPB[14]). Так, 16 травня 2022 року EDPB опублікував для ознайомлення свої рекомендації щодо розрахунку штрафів відповідно до GDPR. Рекомендації включають п’ять кроків для розрахунку штрафів:

(1) Визначення операцій обробки у справі та оцінка застосування статті 83 GDPR;

(2) Знаходження початкової точки для подальших розрахунків;

(3) Оцінка обтяжуючих і пом’якшуючих обставин, пов’язаних із минулою або теперішньою поведінкою контролера/обробника даних, і відповідно збільшення або зменшення штрафу;

[14] The European Data Protection Board. URL: https://www.edpb.europa.eu/edpb_en

(4) Визначення відповідних законодавчих максимумів для різних операцій обробки, відповідно до яких збільшення, застосоване на попередніх або наступних етапах, не може перевищувати цю суму;

(5) Аналіз відповідності остаточної суми розрахованого штрафу вимогам ефективності, стримування та пропорційності, як того вимагає стаття 83 GDPR, і відповідно збільшення або зменшення штрафу. Рекомендації покликані гармонізувати методологію розрахунку штрафів за порушення GDPR та підвищити прозорість у всій Європейській економічній зоні, проте вони вважаються «м'яким правом» і, відповідно, не мають юридичної сили.

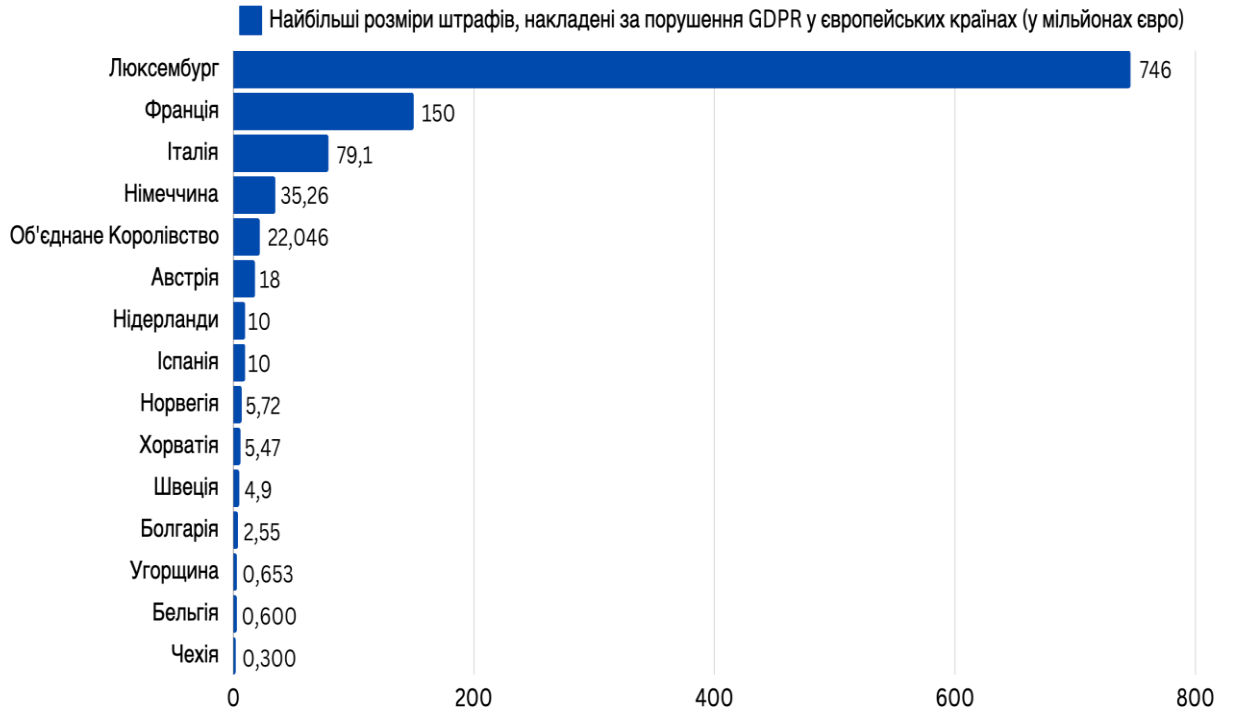
У визначенні фінансових санкцій (штрафів) використовуються загальні вимоги GDPR (два рівні штрафів), персоніфікований підхід до призначення штрафу і доцільність застосування додаткових санкцій, визначених в адміністративному/кримінальному законодавстві. Визначення відповідних розмірів залежить від дискреції уповноваженого контрольно-наглядового органу відповідної держави.

Найбільші розміри штрафів, що були застосовані наглядовими органами (судом), по країнам (2019–2024 рр.), вказують на доволі диференційовані підходи у цьому напрямі[15]:

– Австрія: 18 мільйонів євро – на Австрійську поштову службу («Österreichische Post AG»);
– Бельгія: 600 000 євро – на Google Belgium;
– Болгарія: 2 550 000 євро – на Національне агентство доходів Болгарії («NRA»);
– Іспанія: 10 млн євро – на Google LLC;
– Італія: 79,1 мільйона євро – на Enel Energia SpA;
– Люксембург: 746 млн євро – на Amazon;
– Нідерланди: 10 млн євро – на Uber Technologies Inc. і Uber BV;
– Німеччина: 35,26 млн євро – на H&M;
– Норвегія: 65 млн норвезьких крон – на Grindr LLC;
– Об'єднане Королівство: 22 046 000 євро – на British Airways;
– Угорщина: 653 000 євро – на Будапештський банк;
– Франція: 150 млн євро – на GOOGLE LLC і GOOGLE IRELAND LIMITED;
– Хорватія: 5,47 млн євро – на колекторську агенцію;
– Чехія: 300 000 євро – на транспортну компанію;
– Швеція: 4,9 млн євро – на Spotify (рис. 1).

[15] Дані з відкритого доступу. URL: https://cms.law/en/int/publication/gdpr-enforcement-tracker-report

Рис. 1



Висновки. GDPR змінив підходи до захисту персональних даних: відтепер акцент зміщується із захисту даних корпоративного сектору на захист персональних даних, створення цифрового ринку, де роль ЄС у забезпеченні регулювання є вирішальною. Персональні дані стали новим фактором виробництва та новою валютою змін.

Разом із тим, попри зусилля міжнародних організацій і держав, досконалої системи захисту персональних даних не існує. Кожен механізм захисту, створюваний як на національному, так і на міжнародному рівнях, потребує постійного удосконалення.

Водночас, держави-члени ЄС *користуються розмірами штрафів, передбачених Регламентом GDPR*. На додаток до цих штрафів (фінансових санкцій) національне законодавство низки європейських країн запроваджує додаткові санкції адміністративного/кримінального характеру – за порушення вимог законів про захист персональних даних. Окрім того, можуть застосовуватися коригувальні заходи, зокрема тимчасове припинення (обмеження) для юридичної особи на виконання обробки персональних даних.

Оскільки у європейському законотворенні обрано підхід, за яким *не визначається нижня межа можливого штрафу*, а лише верхня, то визначення суми штрафу залишається дискреційним рішенням

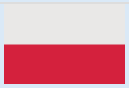
уповноваженого органу (з урахуванням зокрема тяжкості правопорушення). При цьому, у всіх державах штрафи, які накладає уповноважений контролюючий орган (фінансові санкції), є набагато актуальнішими, ніж позови про відшкодування збитків, що випливають із судових розглядів, пов'язаних із порушенням захисту даних.

Дослідницька служба
Верховної Ради України

**Цей документ підготовлений Дослідницькою службою Верховної Ради України як довідковий інформаційно-аналітичний матеріал. Інформація та позиції, викладені в документі, не є офіційною позицією Верховної Ради України, її органів або посадових осіб. Цей документ може бути цитований, відтворений та перекладений для некомерційних цілей за умови відповідного посилання на джерело.*

Додаток 1[16]

Публічна інформація щодо накладення штрафів за порушення GDPR у деяких державах

ETid	Країна	Дата прийняття рішення	Штраф, євро	Контролер/процесор	Цитована норма	Тип порушення
ETid-2372	 ІСПАНІЯ	2024-06-17	600	Balonmano	ст. 6 (1) GDPR	Недостатня правова база для обробки даних
ETid-2371	 ІСПАНІЯ	2024-06-20	42 000	CUI ZSQ FOOD, SL	ст. 5 (1) f) GDPR	Недотримання загальних принципів обробки даних
ETid-2370	 ІТАЛІЯ	2024-05-09	75 000	Azienda ospedale università di Padova	ст. 5 (1) a), c), f) GDPR, ст. 9 GDPR, ст. 25 GDPR, ст. 32 GDPR	Недотримання загальних принципів обробки даних
ETid-2369	 ПОЛЬЩА	2024-04-24	2500	Committee	ст. 5 (1) f) GDPR, ст. 5 (2) GDPR, ст. 25 (1) GDPR, ст. 32 (1), (2) GDPR	Недостатні технічні та організаційні заходи щодо забезпечення інформаційної безпеки
ETid-2364	 ІТАЛІЯ	2024-04-24	3000	INPAS	ст. 5 (1) a) GDPR, ст. 6 GDPR, ст. 9 GDPR, ст. 2-ter Codice della privacy (Кодекс конфіденційності), ст. 2- Codice della privacy	Недостатня правова база для обробки даних
ETid-2303	 ХОРВАТІЯ	2024-04-22	500-4000	Невідомий	ст. 27 Закон Хорватії про імплементацію GDPR, ст. 13 GDPR	Недостатнє виконання зобов'язань щодо інформації

[16] GDPR Enforcement Tracker. URL: https://www.enforcementtracker.com/

ETid-2376	 ROMANIA	2024-06-25	1000	Rețele Electrice Dobrogea SA	ст. 32 (1) b) GDPR, ст. 32 (2) GDPR	Недостатні технічні та організаційні заходи щодо забезпечення інформаційної безпеки
ETid-2347	 ФРАНЦІЯ	2024-06-05	Невідомий	Невідомий	Невідомий	Недостатня співпраця з наглядовим органом
ETid-2317	 ОБ'ЄДНАНЕ КОРОЛІВСТВО	2024-04-30	8700	Central Young Men's Christian Association	ст. 5 (1) f) GDPR, ст. 32 (1), (2) GDPR	Недостатні технічні та організаційні заходи щодо забезпечення інформаційної безпеки
ETid-2309	 НІМЕЧЧИНА	2023	3600	Physician	ст. 5 (1) f) GDPR, ст. 32 (1) b) GDPR	Недостатні технічні та організаційні заходи щодо забезпечення інформаційної безпеки
ETid-2298	 CZECH REPUBLIC	2024-04-15	13,900,000	Avast Software s.r.o.	Невідомий	Невідомий
ETid-2277	 BULGARIA	2023-02-09	5,100	Невідомий	ст. 5 (1) a), b) GDPR, ст. 6 GDPR	Недотримання загальних принципів обробки даних
ETid-2266	 ГРЕЦІЯ	2024-04-02	175 000	Міністерство імміграції та притулку Греції	ст. 25 GDPR, ст. 31 GDPR, ст. 35 GDPR	Недостатні технічні та організаційні заходи щодо забезпечення інформаційної безпеки
ETid-2257	 ІСЛАНДІЯ	2024-03-24	10 000	Stjörnuna ehf	ст. 5 (1) a), b), c) GDPR, ст. 6 GDPR, ст. 12 GDPR, ст. 13 GDPR	Недотримання загальних принципів обробки даних
ETid-2256		2023	50 700	Політична партія	Невідомий	Невідомий

	АВСТРІЯ					
ETid-2247	 КІПР	2023-12-07	1500	Physician	ст. 5 (1) a) GDPR	Недотримання загальних принципів обробки даних
ETid-2199	 НІДЕРЛАНДИ	2023-12-11	10 000 000	Uber Technologies Inc. Uber BV	ст. 12 (1), (2) GDPR, ст. 13 (1) f) GDPR, ст. 13 (2) a), b) GDPR	Недостатнє виконання зобов'язань щодо інформації