Омбудсман України
Ombudsman of Ukraine

Фінансується
Європейським Союзом

FIIAPP
COOPERACIÓN ESPAÑOLA

ВІДПОВІДАЛЬНІСТЬ І САНКЦІЇ ЗА ПОРУШЕННЯ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ (GDPR)

Автор
Олександр Шевчук
експерт проєкту EU4DigitalUA

Проєкт **EU4DigitalUA** є частиною підтримки України Європейським Союзом. Погляди, думки та висновки, висловлені в тексті, належать виключно авторам і не обов›язково представляють позицію проєкту, Європейського Союзу або FIIAPP.

ЗМІСТ

ПЕРЕДМОВА

Особливого значення тема захисту персональних даних набуває для України в контексті інтеграції нашої держави в Єдиний цифровий ринок ЄС та вступу в Європейський Союз.

Договір про асоціацію між Україною та Європейським Союзом вимагає приведення законодавства України у відповідність до європейських стандартів, що стосується також сфери захисту персональних даних. Гармонізація українського законодавства до європейських стандартів у сфері захисту персональних даних шляхом імплементації Регламенту (ЄС) 2016/679 є одним із ключових завдань України відповідно пункту 11 Плану заходів з виконання Угоди про асоціацію, затвердженого Постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106.

Важливо наголосити, що для повноцінного функціонування системи захисту персональних даних в Україні наразі важливим є прийняття законопроекту «Про захист персональних даних» та законопроекту «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації». Прийняття цих законопроектів дасть можливість привести систему захисту персональних даних в Україні у відповідність до Регламенту (ЄС) 2016/679 (GDPR) та Конвенції 108 +.

Слід підкреслити, що Регламент (ЄС) 2016/679 передбачає створення незалежного органу в сфері захисту персональних даних в кожній державі-члені ЄС і надає повноваження наглядовому органу проводити розслідування у випадку порушення безпеки персональних даних і накладати штрафні санкції за порушення. Регламент (ЄС) 2016/679 надає наглядовому органу повноваження з визначення розміру штрафних санкцій, які мають бути «ефективними, пропорційними й стримувальними». Регламент (ЄС) 2016/679 формулює також обтяжувальні й пом'якшувальні обставини, які наглядовий орган має враховувати, визначаючи розмір штрафу.

У зв'язку з цим в українських компаній викликають занепокоєння штрафні санкції і загалом підхід Регламенту (ЄС) 2016/679 до накладення грошових стягнень за порушення, оскільки Регламент (ЄС) 2016/679 слугував дороговказом при розробленні положень обох законопроектів.

Для того, щоб надати можливість українському бізнесу краще зрозуміти:

- як наглядові органи з питань захисту персональних даних ЄС розглядають справи щодо порушення положень Регламенту (ЄС) 2016/679;
- яким чином оцінюють шкоду для суб'єктів персональних даних внаслідок порушення їх прав;
- який алгоритм використовують наглядові органи держав-членів ЄС при накладенні і визначенні розміру штрафних санкцій за порушення безпеки персональних даних відповідно до положень GDPR.

в цьому дослідженні ми проаналізували:

- положення Регламенту (ЄС) 2016/679 щодо відповідальності і штрафних санкцій за порушення;
- механізм розрахунку адміністративних штрафів відповідно до Регламенту (ЄС) 2016/679 (GDPR) згідно Настанови 04/2022, яку ухвалила Європейська рада із захисту даних — EDPB (European Data Protection Board);
- методологію розслідування наглядовим органом справ про порушення національного законодавства в сфері захисту персональних даних на прикладі Республіки Естонія;
- 30 практичних кейсів наглядових органів держав-членів ЄС і Великобританії щодо розгляду порушень різноманітних положень Регламенту (ЄС) 2016/679.

ЗАГАЛЬНИЙ РЕГЛАМЕНТ ПРО ЗАХИСТ ДАНИХ (GDPR)

18 грудня 2015 року Комітет постійних представників у Європейському Союзі (КПП) затвердив текст, узгоджений з Європейським Парламентом щодо реформи захисту персональних даних в Європейському Союзі і вже 14 квітня 2016 року Європейський Парламент схвалив узгоджений текст Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року «Про захист фізичних осіб стосовно обробки особистих даних і про вільне переміщення таких даних», скасувавши попередню Директиву 95/46/ЄС про захист даних 1995 року. Регламент (ЄС) 2016/679 набрав чинності після дворічного перехідного періоду і вступив в силу в травні 2018 року.

Ключовою новелою Регламенту (ЄС) 2016/679 є можливість накладання на компанію грошового стягнення в розмірі до чотирьох відсотків її річного світового обороту (або до 20 000 000 євро, якщо ця сума є більшою) за більш серйозні порушення положень Регламенту (ЄС) 2016/679, або

до двох відсотків її річного світового обороту (або до 10 000 000 євро, якщо ця сума є більшою) за менш серйозні порушення положень Регламенту (ЄС) 2016/679. При вирішенні питання про накладання грошового стягнення і його розмір наглядовий орган з питань захисту персональних даних має враховувати такі обставини як характер, тяжкість і тривалість порушення і його наслідків, заходи, вжиті для забезпечення виконання вимог Регламенту (ЄС) 2016/679 та будь-які заходи, спрямовані на запобігання спричинення порушенням негативних наслідків або на пом'якшення їхнього впливу.

Нові розміри штрафів є, мабуть, одними з найважливіших положень Регламенту (ЄС) 2016/679, які можуть змусити компанії докорінно переглянути свої погляди на питання відповідності вимогам законодавства ЄС в сфері захисту персональних даних та відчути ризик понести реальну відповідальність за порушення положень Регламенту (ЄС) 2016/679 і інвестувати більше ресурсів у системи і механізми безпеки для забезпечення виконання вимог Регламенту (ЄС) 2016/679.

Регламент (ЄС) 2016/679 надає наглядовому органу повноваження щодо визначення розміру штрафних санкцій, які мають бути «ефективними, пропорційними й стримувальними». Регламент (ЄС) 2016/679 формулює також обтяжувальні й пом'якшувальні обставини, які наглядовий орган має враховувати, визначаючи розмір штрафу. Наприклад, умисні порушення є тяжчими за допущені з халатності. Пом'якшувальними обставинами є дотримання кодексу поведінки або стандартів механізму сертифікації і впровадження належних технічних і організаційних заходів захисту персональних даних. У випадку порушення вимог контролер та процесор вправі зменшити розмір штрафу, пом'якшивши «шкідливий характер, тяжкість і тривалість порушення» шляхом оперативного інформування про нього та співпраці з наглядовим органом.

Загальні умови для накладання адміністративних штрафів визначені статтею 83 Регламенту (ЄС) 2016/679.

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

(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 процесором для зниження рівня шкоди, заподіяної суб'єктами даних;

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

(e) будь-які виявлені попередні порушення з боку контролера або процесора;

(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, і яким чином, контролер або процесор повідомив про порушення;

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

(j) дотримання затверджених кодексів поведінки відповідно до статті 40 або затверджених стандартів механізму сертифікації 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 процесор навмисно чи за недбалістю, для тих самих чи пов'язаних операцій опрацювання, порушує декілька положень цього Регламенту, загальна сума адміністративного штрафу не повинна перевищувати суму, визначену для найтяжчого порушення.

Регламент (ЄС) 2016/679 встановлює два рівні максимальних штрафних санкцій в залежності від наявності у контролера і процесора історії порушень і характеру самого порушення. Верхньою межею розміру штрафу є чотири відсотки річного світового обороту компанії або 20 мільйонів євро. Нижньою межею розміру штрафу є два відсотки річного світового обороту компанії або 10 мільйонів євро.

Зокрема, штрафні санкції нижньої межі накладаються за порушення наступних положень Регламенту (ЄС) 2016/679:

(a) обов'язки контролера і процесора 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);

Штрафні санкції верхньої межі накладаються за порушення наступних положень Регламенту (ЄС) 2016/679:

(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).

Положення Регламенту (ЄС) 2016/679 з накладання штрафних санкцій за

порушення запроваджують ефективні механізми невідворотності й послідовності призначення покарання. Суттєві штрафи за порушення не лише стимулюють невідворотність покарання, вони є помітною особливістю Регламенту (ЄС) 2016/679, яка змусила національні й транснаціональні компанії інвестувати більше ресурсів у системи і механізми безпеки для забезпечення виконання вимог Регламенту (ЄС) 2016/679.

МЕХАНІЗМ РОЗРАХУНКУ АДМІНІСТРАТИВНИХ ШТРАФІВ ВІДПОВІДНО ДО ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ (GDPR)

24 травня 2023 року Європейська рада із захисту даних — EDPB (European Data Protection Board) ухвалила Настанови 04/2022 щодо розрахунку адміністративних штрафів відповідно до Загального регламенту захисту даних GDPR (General Data Protection Regulation) з метою гармонізації методології, яку використовують наглядові органи при розрахунку розміру такого штрафу. Ці Настанови доповнюють раніше прийняті Настанови 2016/679 (WP253) щодо застосування та встановлення адміністративних штрафів відповідно до цілей Регламенту, які описують обставини, за яких такий штраф накладається.

Розрахунок суми штрафу здійснюється на розсуд наглядового органу з урахуванням правил, передбачених Регламентом (ЄС) 2016/679. У цьому контексті Регламент (ЄС) 2016/679 вимагає, щоб розмір штрафу в кожному окремому випадку був ефективним, пропорційним і стримуючим (ст. 83(1) GDPR). Крім того, при визначенні розміру штрафу наглядові органи повинні належним чином враховувати перелік обставин, які стосуються особливостей порушення (його серйозності) або особи порушника (ст. 83(2) GDPR). Нарешті, розмір штрафу не повинен перевищувати максимальних сум, передбачених у статтях 83(4), (5) та (6) GDPR. Таким чином, кількісне визначення розміру штрафу ґрунтується на конкретній оцінці, що проводиться в кожному конкретному випадку, в межах параметрів, передбачених Регламентом (ЄС) 2016/679.

Беручи до уваги вищезазначене, для розрахунку адміністративних штрафів за порушення положень Регламенту (ЄС) 2016/679 Європейська рада із захисту даних розробила наступну методологію, що складається з п’яти кроків.

По-перше, необхідно визначити операції з обробки даних у справі та оцінити застосування статті 83(3) GDPR.

По-друге, необхідно визначити відправну точку для подальшого розрахунку суми штрафу. Це робиться шляхом оцінки класифікації порушення в GDPR, оцінки серйозності порушення у світлі обставин справи та оцінки річного обороту суб'єкта господарювання. Третій крок — оцінка обтяжуючих та пом'якшуючих обставин, пов'язаних з минулою або теперішньою поведінкою контролера/процесора інформації, та відповідне збільшення або зменшення штрафу. Четвертий крок — визначення відповідних максимальних розмірів штрафів за різні порушення. Збільшення, що застосовувались на попередніх або будуть застосовуватись на наступному кроці, не можуть перевищувати цю максимальну суму. Нарешті, необхідно проаналізувати, чи відповідає розрахована остаточна сума вимогам ефективності, стримуючого впливу та пропорційності. Штраф все ще може бути скоригований у будь-який бік, але не повинен перевищувати встановлений законом максимальний розмір.

На всіх вищезазначених етапах слід пам'ятати, що розрахунок штрафу не є простою математичною операцією. Саме обставини конкретної справи є визначальними факторами, що впливають на остаточну суму, яка в усіх випадках може бути будь-якою, аж до встановленого законом максимуму включно.

Беручи до уваги ці параметри, Європейська рада із захисту даних розробила наступну методологію розрахунку адміністративних штрафів за порушення положень GDPR.

Крок 1	Ідентифікація операцій з обробки даних у справі та оцінка доцільності застосування статті 83(3) GDPR.
Крок 2	a) класифікація за статтею 83(4) - (6) GDPR; b) серйозність порушення відповідно до статті 83(2)(a), (b) та (g) GDPR; c) річний світовий оборот суб'єкта господарювання як один із важливих елементів, який слід враховувати з метою накладення ефективного, стримуючого та пропорційного штрафу згідно зі статтею 83(1) GDPR.
Крок 3	Оцінка обтяжуючих та пом'якшуючих обставин, пов'язаних з минулою або теперішньою поведінкою контролера/процесора інформації, та відповідне збільшення або зменшення штрафу.
Крок 4	Визначення відповідних законодавчо встановлених максимумів для різних операцій з обробки даних. Збільшення, що застосовувались на попередніх або будуть застосовуватись на наступному кроці, не можуть перевищувати цю суму.
Крок 5	Аналіз того, чи відповідає остаточна сума нарахованого штрафу вимогам ефективності, стримуючого впливу та пропорційності, як того вимагає стаття 83(1) GDPR, та відповідне збільшення або зменшення штрафу.

Крок 1

Ідентифікація операцій обробки даних у справі та оцінка доцільності застосування ст. 83 (3) GDPR. Цей крок допомагає встановити, чи існує одне, чи декілька санкціонованих діянь, а також те, як підходити до ситуацій з декількома порушеннями.

Наприклад, Європейська рада із захисту даних наводить практичні приклади того, як розрізнити, чи йдеться про однакові чи пов'язані операції з обробки даних, або чи можна вважати одне порушення вторинним по відношенню до іншого порушення. Іншим прикладом є єдність дій, коли одна поведінка підпадає під дію кількох законодавчих положень або коли одна дія порушує одне й те саме положення кілька разів.

Крок 2

Встановлення єдиної відправної точки для подальших розрахунків на основі наступних трьох елементів:

- оцінка класифікації порушення відповідно до ст. 83(4)-(6) GDPR;
- серйозність порушення відповідно до ст. 83(2) GDPR, з урахуванням характеру, тяжкості та тривалості порушення. Європейська рада із захисту даних детально роз'яснює, як порушення може мати низький, середній або високий рівень серйозності, виходячи з таких факторів, як характер, обсяг або мета відповідної обробки даних, кількість суб'єктів даних, яких це стосується, і рівень шкоди, якої вони зазнали, а також навмисний або необережний характер порушення та категорії персональних даних, на які впливає порушення. Залежно від встановленого рівня серйозності порушення наглядовий орган визначатиме стартову суму для подальшого розрахунку адміністративного штрафу у відсотках від максимального розміру штрафу (низький рівень серйозності: 0-10%, середній: 10-20%, високий: 20-100%); а також
- річний світовий оборот суб'єкта господарювання з метою накладення ефективного, стримуючого та пропорційного штрафу відповідно до ст. 83 GDPR. Деякі ключові зміни передбачають наступне:
- Європейська рада із захисту даних заявляє, що буде дотримуватися вимог ст. 83 GDPR, GDPR в цілому та усталеної практики Суду ЄС, в якій зазначено, що річний світовий оборот суб'єкта господарювання може свідчити про розмір та економічну потужність суб'єкта господарювання;
- Методичні рекомендації встановлюють різні діапазони річного обороту суб'єкта господарювання для розрахунку будь-якого зменшення розміру штрафу. Порогові значення для цих діапазонів були змінені порівняно з консультаційною версією. Наприклад, для підприємств з річним світовим оборотом до 2 млн. євро наглядові органи можуть зменшити початковий розрахунок до 0,2% від визначеної початкової суми, тоді як для організацій з річним оборотом від 100 до 250 млн. євро визначена початкова сума може бути скоригована до 15% - 50% від цієї початкової суми;

- Нова категорія — підприємства з річним світовим оборотом понад 500 мільйонів євро; для таких підприємств наглядові органи можуть розглянути питання про нарахування штрафу без будь-якого коригування визначеної стартової суми.

Європейська рада із захисту даних зазначає, що ці порогові значення не є остаточними як і не є обов'язковими. Наглядовий орган не зобов'язаний застосовувати ці коригування, якщо це не є необхідним з точки зору ефективності, стримуючого впливу та пропорційності для коригування початкової суми штрафу.

Крок 3

Оцінка обтяжуючих та пом'якшуючих обставин, таких як будь-які дії, вжиті контролером або процесором для зменшення шкоди, завданої суб'єктам даних, ступінь відповідальності контролера або процесора, ступінь співпраці організації з наглядовим органом тощо.

Щодо наявності попередніх порушень, скоєних контролером або процесором, як обтяжуючого фактора, Європейська рада із захисту даних тепер роз'яснює, що попередні порушення — це порушення, вже встановлені до прийняття рішення (або для процедур Глави VII GDPR, до прийняття проекту рішення наглядовим органом відповідно до ст. 60 GDPR).

Європейська рада із захисту даних також зазначає, що ст. 83(2)(k) GDPR є відкритою і допускає будь-які інші обтяжуючі або пом'якшувальні обставини, і може включати всі обґрунтовані міркування щодо правового, соціально-економічного або ринкового контексту, в якому працює відповідний контролер або процесор. Приклади включають економічну вигоду від порушення або початок пандемії, яка радикально змінює способи обробки персональних даних.

Крок 4

Визначення встановлених законом максимальних сум для різних операцій з обробки даних (таким чином, що збільшення, які застосовувались на попередніх кроках або будуть застосовуватись на наступному кроці, не можуть перевищувати цих сум).

На цьому кроці індивідуально розглядаються так звані «динамічні максимальні» суми штрафів відповідно до GDPR (тобто 2% або 4% від загального річного обороту суб'єкта господарювання за попередній фінансовий рік). Європейська рада із захисту даних детально роз'яснює поняття «суб'єкт господарювання» за законодавством ЄС, наводить численні приклади різних корпоративних структур та пояснює, як слід розраховувати річний оборот відповідно до загальносвітової практики.

Крок 5

Оцінка того, чи буде розрахований штраф відповідати вимогам ефективності, стримуючого впливу та пропорційності, а також чи потрібне подальше коригування штрафу. Наприклад, наглядові органи можуть розглянути (відповідно до національного законодавства) можливість зменшення розміру штрафу з урахуванням впливу штрафу на економічну життєздатність

суб'єкта господарювання та конкретного соціально-економічного контексту (наприклад, кризовий стан галузі, зростання безробіття в регіоні або потенційне погіршення ситуації в суміжних галузях економіки).

МЕТОДОЛОГІЯ РОЗСЛІДУВАННЯ НАГЛЯДОВИМ ОРГАНОМ СПРАВ ПРО ПОРУШЕННЯ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА В СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ НА ПРИКЛАДІ РЕСПУБЛІКИ ЕСТОНІЯ[1]

Сфера нагляду

Інспекція з захисту даних — національний орган Естонії з питань захисту персональних даних та доступу до публічної інформації (далі - Інспекція) має наглядову юрисдикцію відповідно до наступних законодавчих актів:

1. Загальний регламент про захист даних ЄС (Регламент (ЄС) 2016/679, GDPR
2. Закон про захист персональних даних: захист даних у правоохоронній сфері відповідно до Директиви ЄС 2016/680 та деяких сфер, які додатково регулюються національним законодавством на додаток до GDPR (журналістика, наука, послуги з перевірки фінансової достовірності тощо)

[1] Інформацію для даного розділу підготували Viljar Peep (ексголова Інспекції захисту даних Республіки Естонія) та Liisa Ojangu (ексголова відділу перевірок Інспекції захисту даних Республіки Естонія)

3. Закон про доступ до публічної інформації: крім доступу до публічної інформації (запити, упереджувальне розкриття), закон Естонії надає юрисдикцію Інспекції в питаннях підтримки обов'язкових веб-сайтів та мобільних застосунків, захисту інформації з обмеженим доступом (крім державної таємниці), а також створення, запуску, реорганізації та припинення діяльності баз даних державного сектору (§ 45).

4. Закон про електронні комунікації: крім захисту персональних даних, Інспекція має юрисдикцію щодо використання контактних даних фізичних та юридичних осіб для електронного прямого маркетингу («юрисдикція щодо спаму», § 103.1).

5. Регламенти ЄС щодо правоохоронних інформаційних систем (Шенгенська інформаційна система, візова інформаційна система, система Eurodac тощо): Інспекція здійснює нагляд за обробкою даних на національному рівні, особливо за правами доступу суб'єктів даних.

Інспекція матиме нові завдання в рамках імплементації Закону ЄС про управління даними (Регламент (ЄС) 2022/868), але проект національного закону про впровадження ще не готовий.

Процесуальні формати наглядових справ

1. Розслідування можливих порушень, зловживань або ризиків — на основі скарг або повідомлень про витік даних, або розпочате ex officio. Це традиційний процесуальний формат, який регулюється насамперед GDPR ЄС (ст. 57(1) f,h, ст. 58) та національним законодавством.

Інспекція розглядає скаргу щодо захисту даних протягом 30 днів, цей термін може бути продовжений до 60 днів. Скарги на доступ до публічної інформації повинні бути розглянуті протягом 10 днів, цей термін може бути продовжений до 30 днів. Продовження строку часто відбувається у справах про захист даних і майже завжди у справах про доступ до публічної інформації.

Наглядова процедура — це передусім письмова процедура (вона також може включати виїзні перевірки). Закон про адміністративну процедуру також дозволяє вирішувати питання на відкритому засіданні (§ 50), але в реальному житті це не використовується. Схожа ситуація і в інших органах влади Північних та Балтійських країн.

Генеральний директор має всі повноваження, покладені на Інспекцію законодавчими актами. У відповідності до кодифікованих правил внутрішнього розпорядку Інспекції, Генеральний директор делегував право підписувати всі процесуальні документи посадовим особам Інспекції. Внутрішній регламент передбачає проведення обговорень в Інспекції у важливих випадках.

На додаток до розслідування, Інспекція розробила додаткові спеціальні формати для розслідування:

2. «Просте» розслідування — якщо йдеться про незначну справу (наприклад, контролер не відповів суб'єкту даних), Інспекція спробує вирішити справу одним листом нагадуванням-попередженням контролеру/процесору, копію якого також отримує скаржник. Зазвичай, одержувача листа навіть не просять надати зворотній зв'язок. Більше ⅓ справ можна вирішити таким чином (підготовка одного документу на одну справу).

3. Аудит — поглиблене розслідування для отримання глибшої картини управління даними у великій/важливій організації (правоохоронні органи, лікарні, страхові компанії тощо) та його впливу на захист персональних даних. Це може бути зроблено спільно з іншим наглядовим органом (кібербезпека, медичний нагляд, захист прав споживачів тощо) - формально має місце дві паралельні наглядові процедури;

4. Порівняльний моніторинг — порівнюється якийсь важливий аспект роботи багатьох організацій. Результати публікуються і оцінюються за кольорами світлофора (це завжди забезпечує високий інтерес ЗМІ). Органи захисту даних країн Балтії намагаються проводити такий моніторинг спільно раз на рік. Моніторинг може спиратися на дані, зібрані автоматизованим інструментом. Європейська рада із захисту даних розробила такий інструмент для перевірки дотримання правил використання файлів cookie на веб-сайтах: *https://www.edpb.europa.eu/news/news/2024/edpb-launches-website-auditing-tool_en*

5. Циркуляри — Інспекція надсилає листи багатьом одержувачам, або застерігаючи від певної неналежної практики, або відзначаючи певну належну практику. У циркулярі можуть бути представлені результати деяких розслідувань/перевірок/моніторингу у відповідному секторі.

Інспекція також бере участь у заходах транскордонного нагляду, що передбачено ст. 56 та Главою VII. Статистично їх кількість можна порівняти з кількістю внутрішніх справ. Технічно для цього використовується Інформаційна система внутрішнього ринку ЄС.

Слідчі повноваження

Слідчі повноваження, а також наглядові санкції (див. наступну таблицю) визначаються наступними законодавчими актами:

GDPR = Регламент (ЄС) 2016/679

IKS = Isikuandmete kaitse seadus = Закон про захист персональних даних, Естонія

AvTS = Avaliku teabe seadus = Закон про доступ до публічної інформації, Естонія

KorS = Korrakaitseseadus = Закон про правоохоронні органи, Естонія

VVS = Vabariigi Valitsuse seadus = Закон про Уряд Республіки Естонія.

Якщо Інспекція здійснює нагляд за іншими адміністративними органами, замість Закону про правоохоронні органи (KorS) використовується Закон про Уряд Республіки (VVS).

	Захист персональних даних	Публічна інформація
1. Вимагати надати інформацію. Згідно з національним законодавством, Інспекція може зупиняти осіб на місці та ставити їм запитання, а також вимагати від них пред'явлення необхідних документів, які вони мають при собі.	Так GDPR 58(1)a; IKS § 57; KorS § 30; VVS § 75.2(1)1-2	Так AvTS § 50; KorS § 30; VVS § 75.2(1)1-2
1a. Робити запити до телекомунікаційних компаній щодо ідентифікаційних даних кінцевого користувача, пов'язаних з ідентифікаційними токенами, що використовуються в публічних мережах електронних комунікацій, за винятком даних, що стосуються факту передачі повідомлень.	Так IKS § 58(2)	Ні
2. Отримувати доступ для перевірки до інформації, приміщень, обладнання, інструментів (а також відчиняти двері, ворота та усувати інші перешкоди для цього)	Так GDPR 58(1) b,e,f; IKS § 57; KorS § 49-51; VVS § 75.2(1)1-2	Так AvTS § 50; KorS § 49-51; VVS § 75.2(1)3,5
3. Викликати особу до службового приміщення Інспекції та просити поліцію **примусово доставити цю особу до установи** (примусовий привід)	Так IKS § 57; KorS § 31	Ні
4. Ідентифікувати особу (встановити особистість людини) З цією метою Інспекція може зупиняти осіб і вимагати від них пред'явлення документа, що посвідчує особу, отримання відомостей, що дозволяють встановити особу, в тому числі інформацію про місце проживання особи, а також отримання біометричних даних для порівняння.	Так IKS § 57; KorS § 32	Так AvTS § 50; KorS § 32

При встановленні особи може застосовуватися прямий примус (сила), якщо це є необхідним для досягнення мети		
5. Заборонити особі перебувати поруч з певною особою або в певному місці, вимагати, щоб вона залишила місце перебування певної особи/певне місце або не наближалася на певну відстань до певної особи/певного місця.	Так IKS § 57; KorS § 44	Ні
6. Накладати штраф за невиконання обов'язків (примусовий штраф) на осіб, зобов'язаних забезпечити використання слідчих повноважень (див. пункти 1-5), - після видачі адміністративного розпорядження. Перед стягненням штрафу необхідно попередити особу. Однак, як правило, попередження виноситься в тому ж розпорядженні. Стягнення штрафу може повторюватися до тих пір, поки не буде виконано зобов'язання, про яке йдеться у розпорядженні. Якщо особа не сплачує штраф, Інспекція надсилає його державному виконавцю (*судовому приставу-виконавцю*) - у цьому випадку особа також повинна сплатити послуги державного виконавця та інші витрати, пов'язані з примусовим виконанням рішення. Докладно це питання розглядається в Законі «Про штрафи за невиконання або неналежне виконання зобов'язань».	Так GDPR 83(5)e, (6); IKS § 60; KorS § 28	Так KorS § 28
9. Застосовувати прямий примус (силу) для забезпечення використання слідчих повноважень (див. пункти 1-5) — після видачі адміністративного розпорядження. Поліція може бути залучена для надання допомоги. Не стосується інших адміністративних органів.	Так KorS § 28	Так KorS § 28

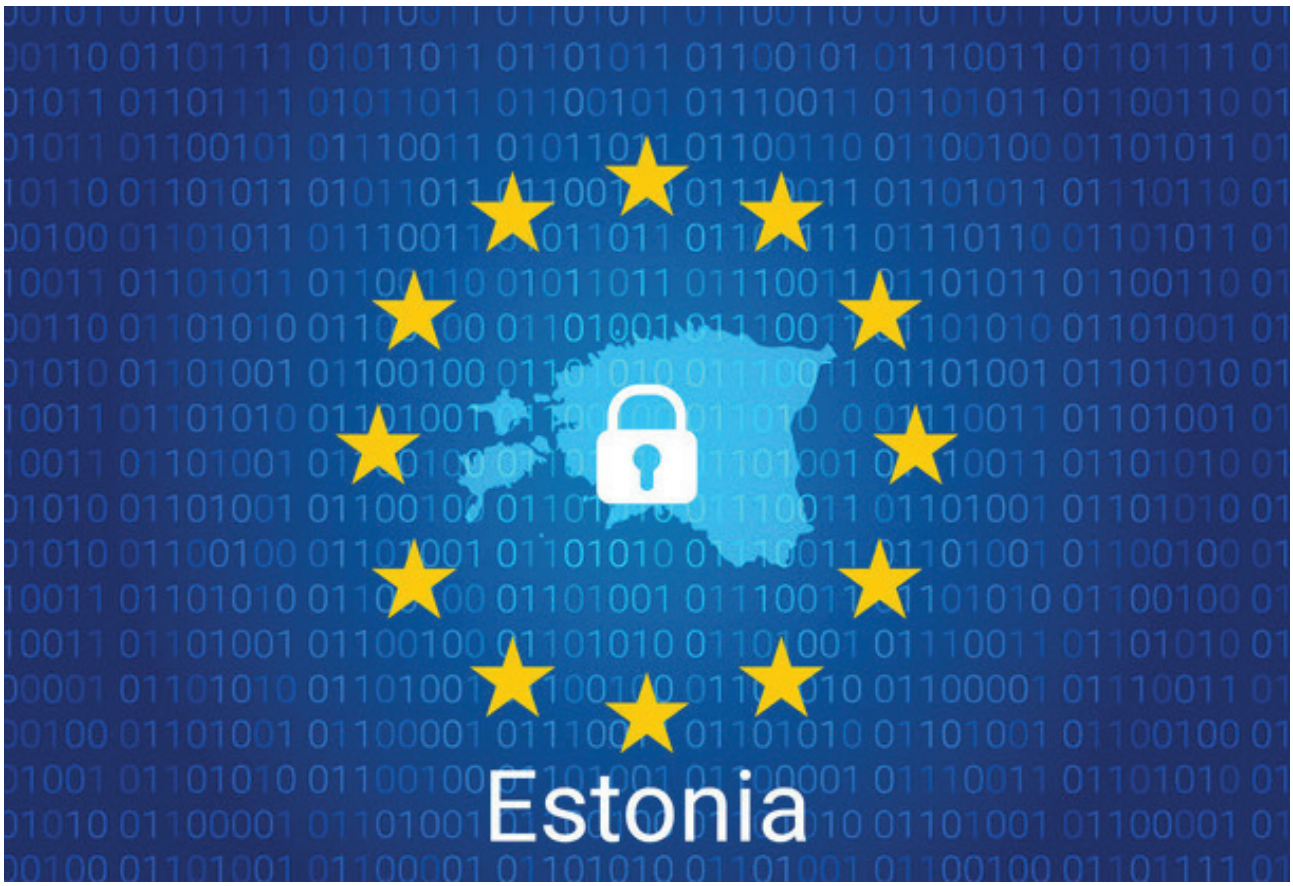
Наглядові санкції

Наглядові санкції не включають покарання (штрафні санкції) за вже вчинені порушення (правопорушення).

	Захист персональних даних	Публічна інформація
1. Попередження. Може бути зроблено без проведення розслідування, превентивно. Може бути адресоване кільком адресатам (формат циркулярів). Закон «Про правоохоронні органи» дозволяє Інспекції попереджати і громадськість. Але якщо підозра виявиться необґрунтованою (особливо якщо вона завдала комусь шкоди), то вона має бути спростована.	Так GDPR 58(2)a; KorS § 26	Так KorS § 26
2. Догана	Так GDPR 58(2)b	Ні
3. Наказ зробити щось або утриматися від чогось.	Так GDPR 58(2)c-h, j	Так AvTS § 51(1)
4. Накладання штрафу за невиконання обов'язків (примусовий штраф) для забезпечення виконання приписаного зобов'язання. Перед стягненням штрафу необхідно попередити особу. Однак, як правило, попередження виноситься в тому ж розпорядженні. Стягнення штрафу може повторюватися до тих пір, поки не буде виконано зобов'язання, про яке йдеться у розпорядженні.	Так GDPR 83(5)e, (6); IKS § 60	Так AvTS § 51(1)

Якщо особа не сплачує штраф, Інспекція надсилає його державному виконавцю — у цьому випадку особа також повинна сплатити послуги державного виконавця та інші витрати, пов'язані з примусовим виконанням рішення.		
5. Якщо орган/посадова особа/працівник державного сектору не виконує розпорядження Інспекції, Інспекція може **звернутися до вищого органу/посадової особи з поданням про проведення службового розслідування або порушення дисциплінарної справи.** Відповідь на подання має бути надана протягом 1 місяця.	Так IKS § 59	Так AvTS § 53
6. Приймати рухоме майно на зберігання.	Так IKS § 57; KorS § 52	Так VVS § 75.2(1)4
7. Продавати або утилізувати рухоме майно, взяте на зберігання. Продаж здійснюється через державного виконавця (судового пристава-виконавця).	Так IKS § 57; KorS § 53	Так VVS § 75.2(1)4
8. Заміщення виконання. У разі невиконання адресатом зобов'язання, Інспекція може виконати зобов'язання за рахунок адресата або організувати виконання зобов'язання третьою особою. Витрати на виконання зобов'язання несе адресат. Якщо він не здійснює оплату, Інспекція направляє його до державного виконавця — тоді особа повинна також сплатити послуги державного виконавця та інші витрати на виконання. Заміна виконання не може бути використана щодо інших державних органів (комунальні підприємства не є державними органами).	Так KorS § 28(2), § 16	Так KorS § 28(2), § 16

9. Застосовувати прямий примус (силу) для забезпечення виконання зобов'язання, що підлягає **примусовому** виконанню. Для цього може бути залучена поліція.	Так KorS § 28	Так KorS § 28
[*10.* ***Подати позов до цивільного суду в Естонії або в іншій державі-члені ЄС.*** *Інспекція може подати масовий позов на захист інтересів великої кількості споживачів до підприємства.* *Таке повноваження передбачено проектом закону естонського парламенту* Ні. 334 SE, який спирається на Директиву ЄС 2020/1828 про представницькі дії для захисту колективних інтересів споживачів].	Законопроект ще не прийнятий.	Ні



Штрафні санкції

У GDPR ЄС спеціально вказується на відсутність **адміністративних штрафів** у двох державах-членах (пункт 151 преамбули). У Данії такі штрафи накладаються судом як кримінальне покарання. В Естонії такі штрафи накладаються в рамках спрощеного кримінального провадження, яке називається **провадженням у справах про проступки** (Кримінально-процесуальний кодекс). Штрафи за проступки здебільшого накладаються адміністративним органом.

Покарання за проступок, призначене адміністративним органом, може бути оскаржене в кримінальному суді 1-го рівня. Але кримінальний суд 2-го рівня виключається. Касаційна скарга може бути подана до 3-ї судової інстанції, але Верховний суд Естонії самостійно вирішує, які скарги він розглядатиме, а які ні.

Вважається, що права оштрафованих осіб є більш захищеними у провадженні у справах про проступки, ніж у наглядовому провадженні. У наглядовому провадженні особи зобов'язані співпрацювати з наглядовим органом — відмова від співпраці може бути санкціонована зборами та штрафами за невиконання вимог. Однак у справі про проступок застосовується принцип кримінального судочинства, згідно з яким ніхто не зобов'язаний свідчити проти самого себе. Отже, у справі про проступок особа не зобов'язана співпрацювати та надавати запитувану інформацію.

Провадження у справі про проступок може бути порушено проти фізичної особи та юридичної особи, а також

проти посадової особи та працівника державного органу — але не проти самого державного органу.

Зазвичай Інспекція відкриває наглядову справу. Якщо є підстави вважати, що відбулося досить суттєве порушення, відкривається справа про проступок. Якщо з самого початку зрозуміло, що в минулому мало місце значне порушення, то з самого початку відкривається справа про проступок.

Важливо відрізняти штраф за проступок від штрафу за невиконання обов'язків. Штраф накладається як покарання за минуле порушення. Якщо порушення все ще триває або існує ризик того, що воно може статися в майбутньому, в цьому випадку Інспекція застосовує штраф за невиконання обов'язків або попередження про застосування штрафу в рамках наглядової справи.

У реальному житті Інспекція застосовує штрафи за проступки як крайній захід (*ultima ratio*), завжди надаючи перевагу наглядовим санкціям, коли це можливо.

Особиста рекомендація автора цього огляду — розглядати штрафні санкції як адміністративні штрафи за порушення адміністративного законодавства, як це роблять 25 країн-членів ЄС і як це робить сьогодні Україна.

Штрафні санкції за порушення у сфері захисту даних та публічної інформації є наступними:

Штрафи за порушення захисту персональних даних, передбачені статтею 83 GDPR підпадають під юрисдикцію Інспекції.
Штрафи за порушення національного законодавства про захист даних. Національні правила встановлюються в питаннях, де згідно з GDPR держава-член може передбачити національні відмінності: обробка персональних даних а) в журналістиці, б) як академічне, художнє або літературне самовираження, в) для потреб наукових та історичних досліджень і національної статистики, г) з метою архівування в суспільних інтересах — підпадає під юрисдикцію Інспекції. [Закон про захист персональних даних, § 68].
Розголошення персональних даних, отриманих в ході професійної діяльності особою, яка за законом зобов'язана не розголошувати таку інформацію, - в юрисдикції поліції. [Кримінальний кодекс, § 157].

Незаконне розголошення або надання можливості незаконного доступу до спеціальних категорій персональних даних та даних про вчинення правопорушення або про те, що особа стала жертвою правопорушення, до початку відкритого судового розгляду або прийняття рішення у справі про правопорушення або до припинення судового провадження у справі підпадають під юрисдикцію Інспекції; у більш серйозних випадках — під юрисдикцію поліції та кримінального суду. [Кримінальний кодекс, § 157.1].
Крадіжка персональних даних підпадає під юрисдикцію поліції та кримінального суду. [Кримінальний кодекс, § 157.2].
Це правопорушення часто пов'язане зі скаргами на захист даних. Оприлюднення недостовірної публічної інформації підпадає під юрисдикцію Інспекції. [Закон про доступ до публічної інформації, § 54.1].
Розкриття або оприлюднення інформації з обмеженим доступом підпадає під юрисдикцію Інспекції. [Закон про доступ до публічної інформації, § 54.1]
Інспекція відповідає як за доступ до публічної інформації, так і за захист *інформації з обмеженим доступом*. Інформація з обмеженим доступом в Естонії = *конфіденційна, таємна або службова інформація* в Україні (Закон України «Про доступ до публічної інформації», статті 6-9). Державна таємниця не входить до сфери дії Закону про доступ до публічної інформації. Порушення державної таємниці знаходиться в юрисдикції Служби внутрішньої безпеки.
Розголошення або передача інформації з обмеженим доступом іноземній державі/організації підпадає під юрисдикцію поліції та кримінального суду. [Кримінальний кодекс, § 243].
Порушення конфіденційності інформації користувача телекомунікаційними компаніями або неповідомлення про це підпадає під юрисдикцію Інспекції. [Закон про електронні комунікації, § 187].
Порушення конфіденційності статистичних даних підпадає під юрисдикцію Інспекції. [Закон про офіційну статистику, § 40]. Захист даних об'єктів статистики — фізичних та юридичних осіб.

Дозвільні процедури

Окрім наглядових справ та штрафних санкцій, Інспекція також відповідає за дозвільні процедури. На додаток до процедур, передбачених GDPR (наприклад, передача даних до третіх країн та інші дозвільні повноваження, передбачені ст. 58(3)), Інспекція уповноважує: - надавати дозвіл на передачу даних до третіх країн. 58(3)), Інспекція дозволяє

1) наукові та історичні дослідження, які базуються на спеціальних категоріях персональних даних, і в науковій сфері немає комітету з етики (щодо персональних даних, які зберігаються в Національному архіві, Національний архів має права комітету з етики)

[Закон Естонії про захист персональних даних, § 6(4)];

2) дослідження для розробки політики міністерствами та іншими органами виконавчої влади, якщо будуть використовуватися персональні дані, які зберігаються в інших міністерствах/відомствах, і таке дослідження не передбачено законом

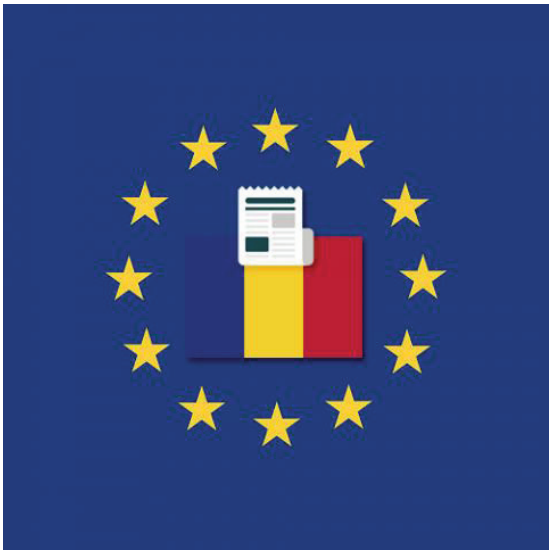
[Закон Естонії про захист персональних даних, § 6(5)];

3) затвердження стандартизованих описів баз даних публічного сектору перед створенням, перед запуском, перед реорганізацією, перед припиненням — спільно з іншими відповідними регуляторами, використовуючи спеціальний портал.

ПРАКТИЧНІ КЕЙСИ

1. ANSPDCP (Румунія)[2]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний акт:	Стаття 58(1)(a) GDPR Стаття 58(1)(e) GDPR Стаття 58(2)(d) GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	31.01.2024



Резюме справи

Наглядовий орган з питань захисту персональних даних Румунії ініціював розслідування щодо місцевого муніципалітету міста Бухарест (контролера) після отримання кількох звернень стосовно можливого порушення положень GDPR.

Повідомлення стосувалися програми «Місцеві заходи із забезпечення енергетичних потреб та підвищення енергоефективності в домогосподарствах». Рішеннями місцевої ради було встановлено, яким чином жителі можуть подати необхідні документи, щоб скористатися фінансовими заохоченнями програми: персонально чи електронною поштою. Однак контролер також зробив доступною онлайн-платформу для збору даних.

Під час розслідування контролер не відповів на неодноразові запити наглядового органу щодо надання інформації відповідно до положень статті 58(1)(a) і (e) GDPR , що призвело до того, що наглядовий орган виніс контролеру попередження.

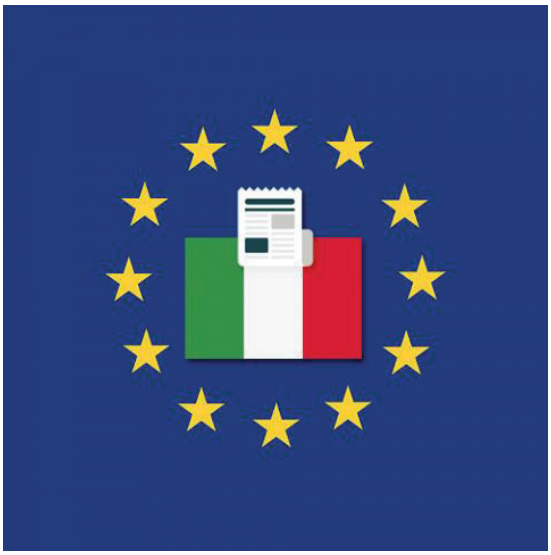
Оскільки контролер не виконав заходи згідно з планом усунення недоліків у встановлений наглядовим органом термін і контролер не відповів на запит наглядового органу щодо надання

[2] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_31.01.2024*

відповідних документів та інформації, останній наклав штраф на контролера у розмірі 2010,38 євро за недотримання положень статті 58(1)(a) і (e) GDPR.

2. Garante per la protezione dei dati personali (Італія)[3]

Наглядовий орган:	Garante per la protezione dei dati personali (Італія)
Юрисдикція:	Італія
Відповідний акт:	Стаття 5(1)(f) GDPR Стаття 9(1) GDPR Стаття 32 GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	30.11.2023



Резюме справи

CB Sistemi srl (процесор) надала постачальнику медичних послуг Medical Center srl (контролер) доступ до результатів медичних досліджень через процес автентифікації.

Особа зайшла на платформу StudioWEB за допомогою облікових даних своєї бабусі. Потім він виявив вразливість системи, яка дозволяла пацієнтам, які ввійшли в систему, отримати доступ до інших звітів, змінивши URL-посилання. Зокрема, особа підкреслила, що змінивши кінцевий номер URL-посилання, можна було отримати доступ до звітів інших пацієнтів. Також можна було навіть переглянути «журнал подій» звіту, який показував список користувачів, які завантажили звіт.

Таким чином, особа повідомила як контролера, так і наглядовий орган з питань захисту персональних даних Італії про вразливість системи. Процесор негайно усунув вразливість системи, а пізніше пояснив, що вона була пов'язана з помилкою, яка виникла під час оновлення програмного забезпечення.

Наглядовий орган звернувся до контролера з проханням надати додаткову інформацію з цього питання.

Наглядовий орган постановив, що медичні звіти, представлені на платформі, можуть розглядатися як дані

[3] *https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9973790*

про стан здоров'я відповідно до статті 4(15) GDPR.

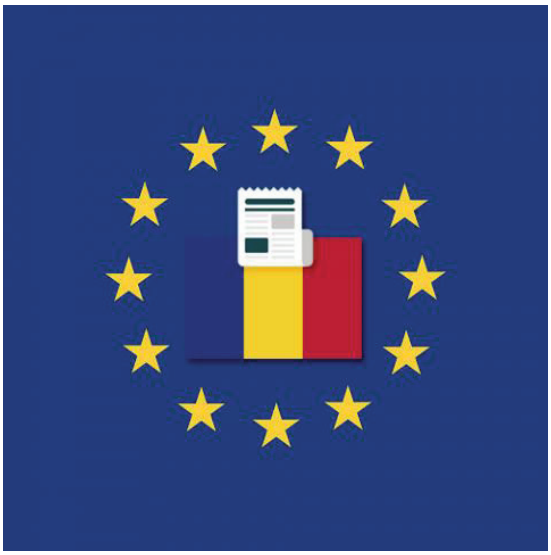
У зв'язку з цим наглядовий орган зазначив, що вразливість системи мала бути передбачена на початковому етапі тестування системи та належним чином виправлена.

Отже, оскільки процесор не взяв до уваги вразливість системи після оновлення програмного забезпечення, наглядовий орган вважав, що процесор не вжив належних заходів для гарантування рівня безпеки, адекватного ризику, як це передбачено статтею 5(1) (f) GDPR і статтею 32 GDPR для забезпечення конфіденційності, цілісності, доступності та стійкості систем обробки та послуг на постійній основі.

Наглядовий орган визнав порушення незначним через обмежений обсяг витоку даних, співпрацю процесора з наглядовим органом під час розслідування та той факт, що вразливість системи була швидко усунена. Таким чином, наглядовий орган не наклав штраф і оголосив процесору догану.

3. ANSPDCP (Румунія)[4]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 5 GDPR Стаття 6(1) GDPR Стаття 9(2) GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	31.08.2023
Штраф:	2000 євро



Резюме справи

Лікар записав пацієнта лікарні, в якій він працював, на свій особистий телефон, а потім опублікував відео на своїй сторінці у соціальній мережі Facebook. Запис проводився без згоди пацієнта. Лікар видалив відео зі своєї сторінки у Facebook в той же день, коли його завантажив.

[4] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_to_a_physician_for_recording_a_patient_on_his_personal_telephone*

За фактом подання скарги до наглядового органу було розпочато розслідування.

Під час розслідування наглядовий орган встановив, що запис лікаря та подальший допис на його сторінці у соціальній мережі Facebook розкрили персональні дані пацієнта, включаючи його зображення, голос, ім'я, прізвище та стан здоров'я. Цей допис побачила велика кількість людей, а також інформація з допису була оприлюднена на різних веб-сайтах і в ЗМІ.

Наглядовий орган оцінював порушення положень GDPR разом із національним законодавством про права пацієнтів. Зокрема, він взяв до уваги статтю 20 Закону 46/2023, яка встановлює, що пацієнта не можна фотографувати чи знімати на відео в медичному закладі без його згоди, за винятком випадків, коли зображення необхідні для діагностики лікування та з метою запобігання підозри про медичну помилку.

Наглядовий орган виявив порушення статті 5 GDPR , статті 6(1) GDPR і статті 9 GDPR. Стаття 5 GDPR встановлює принципи обробки даних персональних даних.

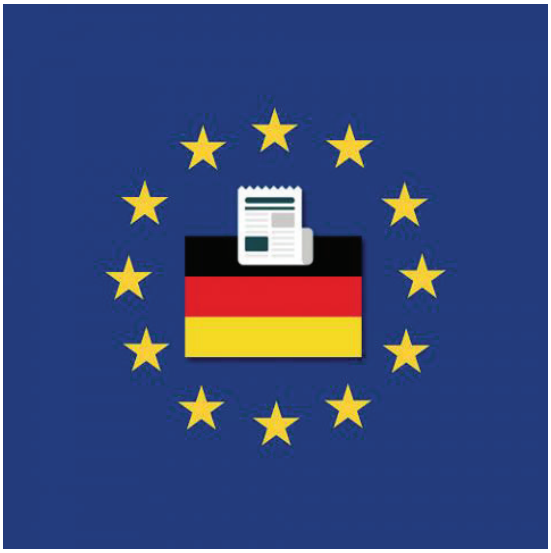
По-перше, стаття 5(1)(a) GDPR встановлює, що персональні дані мають оброблятися у законний, правомірний і прозорий спосіб щодо суб'єкта даних. Обробка персональних даних може бути законною, лише якщо вона здійснюється відповідно до однієї із правових підстав, викладених у статті 6(1) GDPR. З огляду на те, що обробка даних (зйомка та публікація) не мала жодних правових підстав відповідно до статті 6 (1) GDPR, а також була незаконною згідно з національним законодавством, наглядовий орган визнав порушення статті 5 GDPR та статті 6(1) GDPR.

По-друге, стаття 9(2)(a) GDPR встановлює виключення з заборони на опрацювання чутливих категорій персональних даних, наприклад, якщо суб'єкт даних надав явну згоду на опрацювання таких персональних даних для однієї чи декількох визначених цілей, за винятком, якщо законодавством Союзу чи держави-члена передбачено, що суб'єкт даних не може зняти заборону, вказану в параграфі 1;. Дані про здоров'я відносяться до чутливих категорій персональних даних відповідно до статті 9 (1) GDPR. Запис лікаря на особистий телефон демонстрував стан здоров'я пацієнта і був зроблений без його явної згоди пацієнта, що було порушенням статті 9 GDPR.

У результаті виявлених наглядовим органом порушень лікар був оштрафований на 9919,2 RON (еквівалент 2000 євро).

4. ArbG Дуйсбург[5]

Суд:	ArbG Дуйсбург (Німеччина)
Юрисдикція:	Німеччина
Відповідний закон:	Стаття 9 GDPR Стаття 82(1) GDPR
Дата рішення:	16.12.2024



Резюме справи

Контролер був президентом великої асоціації клубів авіаційного спорту («асоціація»), а суб'єкт даних був співробітником цієї асоціації.

11 травня 2023 року суб'єкт даних написав електронний лист 24 особам, у тому числі контролеру, у якому суб'єкт даних, серед іншого, зазначив інформацію про стан свого здоров'я. Як президент асоціації, 11 червня 2023 року, контролер надіслав усім (майже 10 000) членам асоціації циркуляр, в якому зазначено, що суб'єкт даних, незважаючи на те, що з листопада 2022 року перебуває на лікарняному, висунув необґрунтовані звинувачення проти контролера.

6 червня 2023 року контролер припинив трудові відносини із суб'єктом даних. Однак згодом контролера було знято з посади президента асоціації. Після цього суб'єкт даних відновила свою роботу в асоціації.

Циркуляр надісланий контролером усім членам асоціації справив негативний вплив на життя суб'єкта даних. Зокрема, коли суб'єкт даних познайомився з новими людьми з численних спортивних авіаклубів, пов'язаних з асоціацією, він зіткнувся з тим, що вони обізнані з циркуляром контролера про нього.

Суб'єкт даних вимагав від контролера принаймні 17 000 євро відшкодування моральної шкоди за приниження його гідності шляхом публікації конфіденційних даних, а саме інформації про його хворобу та її тривалість. Крім того, суб'єкт даних стверджував, що контролер створив враження, ніби суб'єкт даних завдає шкоди асоціації, навмисно «вдаючи хворого».

Суд постановив, що суб'єкт даних має право на компенсацію в розмірі 10 000 євро від контролера відповідно до статті 82(1) GDPR.

Суд постановив, що надіславши циркуляр всім членам асоціації контролер порушуючи положення статті 9(1) GDPR незаконно здійснивши обробку спеціальних категорій персональних даних (дані про здоров'я) суб'єкта даних.

[5] *https://gdprhub.eu/index.php?title=ArbG_Duisburg_-_3_Ca_77/24*

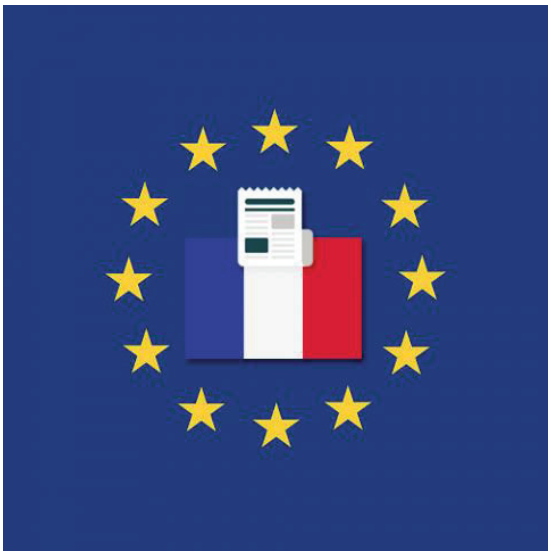
Зокрема, суд постановив, що особистий електронний лист суб'єкта даних від 11 травня 2023 року визначеній групі осіб не можна розглядати як згоду на розкриття інформації контролером. Навіть якщо адресати, визначені суб'єктом даних, частково відповідають адресатам, вибраним контролером у своєму циркулярі від 11 червня 2023 року, це ні за яких обставин не означає згоду суб'єкта даних контролеру надіслати дані про його стан здоров'я.

Суд стверджував, що, беручи до уваги цілі GDPR, відшкодування моральної шкоди в рамках статті 82(1) GDPR слід тлумачити широко. Суд обґрунтував моральну шкоду суб'єкта даних тим фактом, що всі з майже 10 000 членів асоціації дізналися про його хворобу, тривалість його хвороби та ймовірне симулювання його хвороби, що мало вплив на суб'єкта даних, як на роботі, а також у особистому житті.

Суд зазначив, що стаття 82(1) GDPR означає, що позов про відшкодування збитків, передбачений цим положенням, має компенсаційну функцію і не виконує вимог каральної функції. Таким чином, суд визнав компенсацію в розмірі 10 000 євро належною та достатньою, беручи до уваги характер розкритих даних про здоров'я як спеціальних категорій персональних даних (чутливі дані) згідно зі статтею 9 GDPR та ступінь порушення, а саме розкриття інформації майже 10 000 членам асоціації.

5. CNIL (Франція)[6]

Наглядовий орган:	CNIL (Франція)
Юрисдикція:	Франція
Відповідний закон:	Стаття 82 Закону Республіки Франція «Про захист персональних даних» Стаття L. 34-5 Кодексу електронних комунікацій Республіки Франція
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	10.12.2024
Штраф:	50 000 000 євро



[6] *https://gdprhub.eu/index.php?title=CNIL_(France)_-_SAN-2024-019*

Резюме справи

Відповідач надає послугу використання електронної пошти під назвою «Mail Orange» для понад 7 800 000 користувачів і є провідним телекомунікаційним оператором у Франції. Під час службового розслідування Національна комісія у справах інформаційних технологій і прав людини (CNIL) виявила наступне:

У період з 7 по 12 червня 2023 року користувачі зіткнулися з рекламними оголошеннями, які відображалися в їхніх поштових скриньках, як звичайні електронні листи. Єдина відмінність від звичайних електронних листів полягала в тому, що реклама відображалася світло-сірого кольору, містила слово «publicite» і хрестик для миттєвого видалення з електронної пошти. Крім того, було виявлено, що відповідач керував файлами cookie на пристроях користувачів, якщо вони погоджувалися на це.

Аргументи відповідача

Відповідач стверджував, що досі CNIL завжди покладав відповідальність за отримання згоди суб'єкта даних за розміщення реклами на рекламодавця. Тому він не вважав себе відповідальним за отримання згоди, оскільки він просто передав електронну пошту рекламодавця суб'єкту даних, як і звичайні електронні листи. Крім того, він пояснив, що використовував систему, яка дозволяла розповсюджувати рекламні електронні листи без обробки електронної адреси суб'єкта даних.

Файли cookie

Коли користувачі відкликали свою згоду на розміщення файлів cookie на своєму пристрої, файли cookie, які раніше були активовані, продовжували працювати. В цьому випадку відповідач стверджував, що дані, зібрані через файли cookie після відкликання згоди, відповідач в подальшому не обробляв.

Вимога згоди

CNIL у своєму рішенні посилався на рішенні Суду ЄС C-102/20 , яке показало, що електронні листи із рекламним вмістом є прямим маркетингом, який, у свою чергу, вимагає згоди суб'єкта даних. Таким чином, CNIL дійшов висновку, що в цьому випадку відповідно до статті L. 34-5 Кодексу електронних комунікацій Республіки Франція, яка частково імплементує Директиву Європейського Парламенту і Ради 2002/58/ЄС від 12 липня 2002 року щодо опрацювання персональних даних і захисту приватності в секторі електронних комунікацій (Директива про приватність та електронні комунікації) у французьке законодавство, користувачі мають надавати згоду на ці рекламні електронні листи.

Відповідальність відповідача

CNIL постановив, що відповідач як постачальник послуг електронної пошти продає рекламодавцям місця у вхідних повідомленнях своїх користувачів. Оскільки відповідач визначає відображення цих електронних листів, він єдиний, хто безпосередньо контактує з одержувачами електронних листів. Таким чином, це єдина організація, яка могла отримати згоду одержувачів і CNIL в цьому випадку визначив відповідача контролером даних.

Файли cookie

CNIL постановив, що функціонування файлів cookie після відкликання згоди користувача прямо заборонено статтею 82 Закону Республіки Франція «Про захист персональних даних». CNIL заявив, що не має значення, чи підлягали потім отримані дані подальшій обробці відповідачем.

Адміністративний штраф

За порушення статті 82 Закону Республіки Франція «Про захист персональних даних», статті L. 34-5 Кодексу електронних комунікацій Республіки Франція CNIL наклав штраф у розмірі 50 000 000 євро на основі загального річного обігу відповідача. Крім того, CNIL видав наказ припинити незаконну роботу файлів cookie протягом трьох місяців. У разі затримки відповідач має сплатити штраф у розмірі 100 000 євро на день.

6. BAC (Болгарія)[7]

Суд:	BAC (Болгарія)
Юрисдикція:	Болгарія
Відповідний закон:	Стаття 6(1)(b) GDPR Стаття 6(1)(c) GDPR Стаття 6(1)(e) GDPR
Дата рішення:	05.12.2024

Резюме справи

Toplofikacia Sofia EAD (контролер) - болгарська компанія, яка надає послуги постачання теплової енергії своїм клієнтам, як фізичним особам, так і компаніям, у місті Софія. Контролер подав до Міністерства регіонального розвитку Республіки Болгарія запит на доступ до реєстрів персональних даних населення Республіки Болгарія. Причиною запиту було те, що доступ полегшить виконання контрактів між контролером та його клієнтами.

Міністерство регіонального розвитку відмовилося надати доступ до реєстрів, які зберігають значну кількість персональних даних і порадило контролеру згідно зі статтею 125 (3) Закону Республіки Болгарія «Про енергетику» звернутися за дозволом до служ-

[7] *https://gdprhub.eu/index.php?title=%D0%92%D0%90%D0%A1_-_BAC_(Bulgaria)_-_2862/2024*

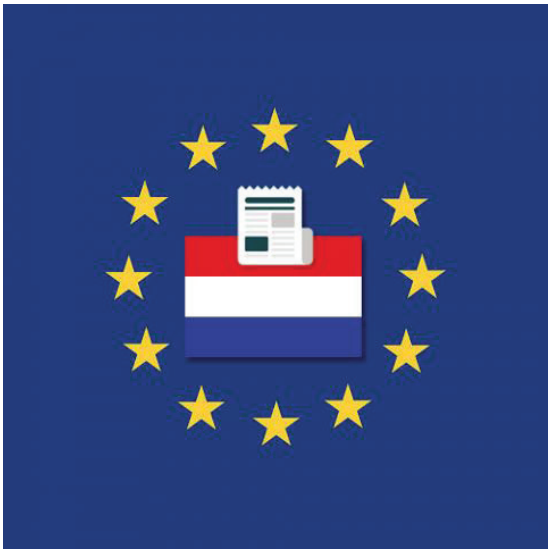
би з питань захисту персональних даних Республіки Болгарія.

У травні 2022 року контролер подав до служби з питань захисту персональних даних Республіки Болгарія заяву про скасування рішення Міністерства регіонального розвитку Республіки Болгарія. У своєму запиті компанія посилалася на статтю 6(1)(b) (обробка є необхідною для виконання контракту, стороною якого є суб'єкт даних, або для вжиття дій на запит суб'єкта даних до укладення договору) GDPR, статтю 6(1)(c) (обробка є необхідною для дотримання встановленого законом зобов'язання, яке поширюється на контролера) GDPR та статтю 6(1)(e) (опрацювання є необхідним для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера) GDPR щодо запиту на доступ до реєстрів.

Наглядовий орган з питань захисту персональних даних Республіки Болгарія провів відповідний аналіз кожної з цих правових підстав і вирішив, що жодна з них не застосовується до контролера. Наглядовий орган відмовився надати доступ до реєстрів і доручив компанії надати відповідне обґрунтування для будь-яких майбутніх запитів до Міністерства регіонального розвитку Республіки Болгарія.

7. AP (Нідерланди)[8]

Наглядовий орган:	AP (Нідерланди)
Юрисдикція:	Нідерланди
Відповідний акт:	Стаття 44 GDPR Стаття 46 GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	26.11.2024



Резюме справи

Суб'єкт даних, якого представляє європейський центр цифрових прав (Noyb), подав скаргу до наглядового органу з питань захисту даних Нідерландів проти контролера, нідерландської компанії доставки їжі Takeaway BV, оскільки вони передали персональні дані суб'єкта даних до США без використання належного механізму транскордонної передачі відповідно до глави V GDPR (передача персональних даних до третіх країн або міжнародних організацій).

[8] *https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_Takeaway_B.V._-_z2022-04011*

У своєму розслідуванні наглядовий орган виявив, що протягом приблизно трьох років контролер використовував Google Analytics (сервіс від компанії Google для аналізу інтернет-сайтів та мобільних додатків) для відстеження та оптимізації функціонування своїх веб-сайтів. Згодом контролер передав дані, такі як унікальні онлайн-ідентифікатори відвідувачів та ідентифікатори файлів cookie на сервери Google Analytics у США

Контролер не заперечував факт передачі персональних даних до Сполучених Штатів на підставі укладено договору із Google LLC (процесором), але наводив наступні аргументи:

Контролер стверджував, що при оцінці рівня захисту персональних даних у США слід використовувати підхід, заснований на оцінці ризику. Оскільки контролер виявив низький ризик при передачі даних, він вважав, що застосовані заходи безпеки є достатніми. Відповідно, належне виконання контролером такого механізму транскордонної передачі даних як стандартні договірні положення (SCC - Standard Contractual Clauses) із процесором є достатнім механізмом для безпечної передачі даних у цій ситуації.

Наглядовий орган при розслідуванні цієї ситуації дійшов висновку, що контролер несе відповідальність за дотримання статті 5(2) GDPR (принцип підзвітності) . Ця відповідальність залишається навіть тоді, коли обробка даних здійснюється процесором або субпроцесором відповідно до статті 28(1) GDPR. Тому контролер несе відповідальність за наявність належного механізму транскордонної передачі даних, навіть якщо передачу здійснював їхній процесор.

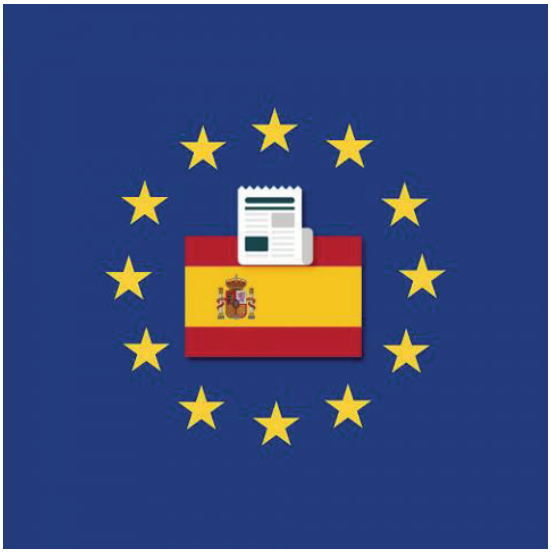
Наглядовий орган постановив, що Google LLC кваліфікується як постачальник електронних комунікаційних послуг і підлягає нагляду американських розвідувальних служб США.

Наглядовий орган підкреслив, що контролер і процесор не вжили достатніх додаткових заходів безпеки при передачі даних, щоб запобігти можливості розвідувальних служб США отримати доступ до цих даних. Наглядовий орган визнав використання проксі-сервера для виключення прямого контакту між відвідувачами веб-сайту та веб-сайтами Google недостатнім, щоб виключити повторну ідентифікацію, враховуючи обсяг даних у Google і можливості спецслужб США. Тому контролер не міг покладатися на SCC (Standard Contractual Clauses) як на інструмент для передачі даних відповідно до статті 46 GDPR.

У зв'язку з цим наглядовий орган оголосив догану контролеру. Хоча він визнав порушення обтяжуючим за статтею 83(2)(a) GDPR, він врахував «конкретну ситуацію» після рішення у справі Schrems II та спроби контролера посилити захист за допомогою проксі-сервера як пом'якшувальні фактори відповідно до статті 83(2)(k) GDPR.

8. AEPD (Іспанія)[9]

Наглядовий орган:	AEPD (Іспанія)
Юрисдикція:	Іспанія
Відповідний закон:	Стаття 6(1) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	24.11.2024
Штраф:	5 000 євро



Резюме справи

Суб'єкт даних працював у компанії Roca & Asociados, (контролер) з 13 березня по 21 липня 2023 року. Контролер опублікував імена та фотографії своїх співробітників без їхньої згоди на веб-сайті компанії.

21 серпня 2023 року суб'єкт даних подав скаргу до Іспанського агентства із захисту персональних даних (AEPD) на контролера.

Контролер заперечив проти звинувачення, заявивши, що суб'єкт даних погодився на публікацію свого фото, позуючи для фото та надавши деталі зі свого резюме для використання в розділі профілю фірми. Компанія надіслала електронний лист співробітникам, щоб підготуватися до фотозйомки. Контролер додав до своєї аргументації, що суб'єкт даних опублікував ті самі дані у своєму профілі LinkedIn.

AEPD підтвердило, що контролер в якості підстави для обробки персональних даних посилався на згоду суб'єкта даних.

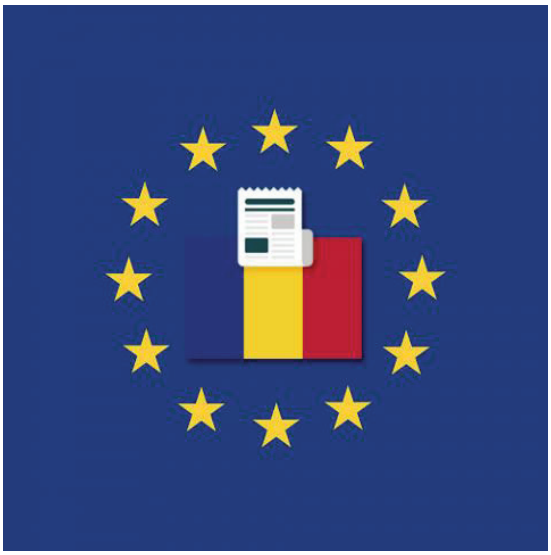
Стосовно визначення згоди згідно зі статтею 4(11) GDPR, AEPD підкреслило, що суб'єкт даних повинен бути належним чином проінформований про обробку та надати чітку і ствердну згоду. Під час свого розслідування AEPD не виявило доказів чіткої заяви суб'єкта даних про те, що він погодився на обробку його персональних даних у формі публікації на веб-сайті.

AEPD постановило, що контролер лише припустив згоду суб'єкта даних, що не відповідає вимогам згоди щодо чітких ствердних дій суб'єкта даних. Тому наглядовий орган виявив порушення статті 6(1) GDPR і наклав на контролера штраф у розмірі 5000 євро.

[9] *https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202313226*

9. ANSPDCP (Румунія)[10]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 58(1)(a) GDPR
Тип справи:	Скарга
Результат:	Підтримано
Дата рішення:	06.08.2024
Штраф:	4977,10 RON



Резюме справи

Суб'єкт даних отримував небажані телефонні дзвінки комерційного характеру від контролера. Після цього він подав контролеру запит на видалення даних.

Однак контролер так і не відповів на цей запит і продовжував здійснювати телефонні дзвінки.

Тому суб'єкт даних подав скаргу до наглядового органу з питань захисту персональних даних Румунії. Наглядовий орган зобов'язав контролера надати інформацію відповідно до статті 58(1)(a) GDPR. Проте, на звернення від наглядового органу контролер не відповів.

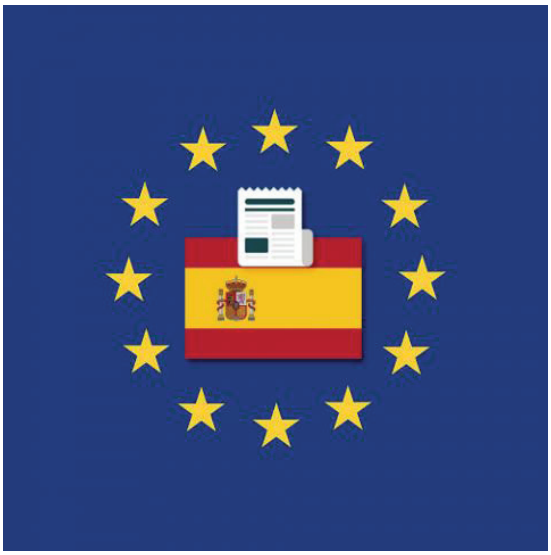
У наглядовому органі зазначили, що контролер не відповів на його розпорядження щодо надання інформації про поточну обробку даних. Тому він виявив порушення статті 58(1)(a) GDPR.

На цій підставі він наклав штраф на контролера у розмірі 1000 євро (4977,10 леїв).

[10] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_BEST_ELAN_ONLINE_SRL*

10. AEPD (Іспанія)[11]

Наглядовий орган:	AEPD (Іспанія)
Юрисдикція:	Іспанія
Відповідний закон:	Стаття 21 Закону Іспанії "Про послуги інформаційного суспільства та електронну комерцію"
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	20.11.2024
Штраф:	20 000 євро



Резюме справи

2 січня 2024 року суб'єкт даних подав скаргу на контролера - Supervista Optics до Іспанського агентства із захисту персональних даних (AEPD). Суб'єкт даних отримав електронний лист від контролера, в якому повідомлялося, що хоча минуло два роки з моменту придбання окулярів у контролера, вона має право на безкоштовний огляд очей у контролера.

Раніше, 24 травня 2023 року, суб'єкт даних скористався своїм правом відмовитися від отримання будь-яких маркетингових повідомлень. Контролер підтвердив отримання запиту та помістив суб'єкта даних до «маркетингового чорного списку».

Контролер стверджував, що повідомлення було електронним листом, у якому не розглядався вміст комерційного характеру. У ньому було зазначено, що було виправдано надіслати цей електронний лист, оскільки гарантія на придбані окуляри ще не закінчилася. Він також стверджував, що стаття 21 Закону Іспанії "Про послуги інформаційного суспільства та електронну комерцію", який прийнято з метою імплементації в національне законодавство положень Директиви Європейського Парламенту і Ради 2002/58/ЄС від 12 липня 2002 року щодо опрацювання персональних даних і захисту приватності в секторі електронних комунікацій (Директива про приватність та електронні комунікації), дозволяє розміщувати комерційну рекламу за умови наявності договірних відносин між контролером і суб'єктом даних.

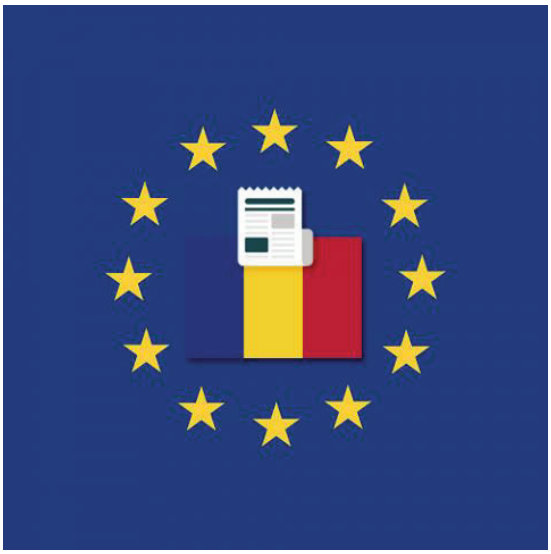
[11] *https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202401934*

AEPD постановило, що будь-яка форма комунікації, яка прямо чи опосередковано рекламує товари чи послуги компанії, класифікується як така, що має комерційний характер. Незважаючи на те, що запропонована послуга є безкоштовною, вона виконується в рамках комерційної діяльності контролера.

AEPD призначило штраф у розмірі 20 000 євро за порушення 21 (1) Закону Іспанії "Про послуги інформаційного суспільства та електронну комерцію".

11. ANSPDCP (Румунія)[12]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 32(1)(b) GDPR Стаття 32(2) GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	18.11.2024
Штраф:	20 000 євро



Резюме справи

Контролер - онлайн-продавець електроніки був поінформований третьою стороною про те, що облікові дані деяких суб'єктів даних були опубліковані в Інтернеті. Ці дані включали ім'я, прізвище, електронну пошту, а також інформацію, доступну в обліковому записі клієнта, таку як адреса доставки, номер телефону, історія замовлень і дані, пов'язані з картками, за допомогою яких здійснювалися онлайн-платежі.

Крім того, контролер встановив, що такі дані (ім'я, прізвище, номер телефону, ...) були оприлюднені в Інтернеті через так званий «credential stuffing», тобто незаконну дію, яка полягає у використанні викрадених ідентифікаторів користувачів і відповідних паролів для того, щоб отримати доступ до облікових записів суб'єктів даних на платформі контролера.

Контролер повідомив про ці порушення даних наглядовому органу з питань захисту персональних даних Румунії.

Наглядовий орган дійшов висновку, що контролер не вжив належних захо-

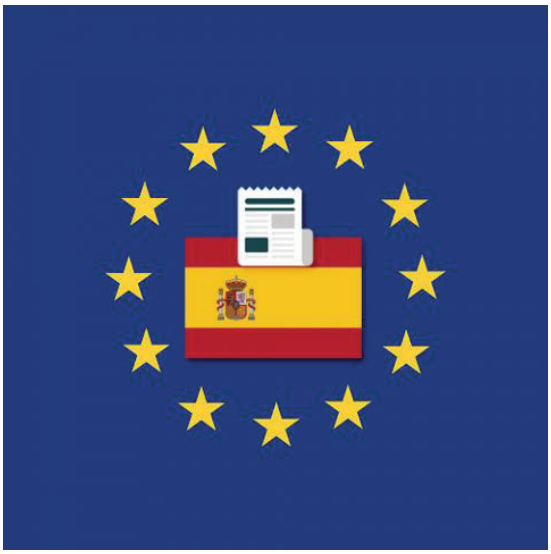
[12] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_Altex_Romania_S.A.*

дів безпеки для запобігання несанкціонованому доступу до персональних даних користувачів, порушивши статті 32(1)(b) і 32(2) GDPR .

На цих підставах наглядовий орган наклав штраф на контролера у розмірі 99 516 лей (20 000 євро) і зобов'язав запроваджувати сповіщення про вхід на нові пристрої, відображати в облікових записах пристрої, на яких виконано вхід, і застосовувати складні політики паролів для всіх облікових записів клієнтів.

12. AEPD (Іспанія)[13]

Наглядовий орган:	AEPD (Іспанія)
Юрисдикція:	Іспанія
Відповідний закон:	Стаття 5(1)(f) GDPR Стаття 63 GDPR Стаття 4.7 та 5.1(f) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	15.11.2024
Штраф:	2000 євро



Резюме справи

Суб'єкт даних подав скаргу до Іспанського агентства із захисту персональних даних (AEPD) проти Blu Management Spain, SL, агентства з підбору персоналу, стверджуючи про несанкціоноване розкриття її персональних даних. Згідно зі скаргою, суб'єкт даних зв'язався з агентством у травні 2023 року та взяв участь у телефонному інтерв'ю. Згодом вона отримала кілька повідомлень у WhatsApp від третьої сторони, яка стверджувала, що інтерв'юер у агентстві Blu Management Spain, SL поділився її ім'ям і номером телефону.

Суб'єкт даних звернулася до агентства, щоб дізнатися про несанкціоноване розголошення її персональних даних, і подала запит на видалення даних, так і запит на доступ до даних. У відповідь контролер заявив, що володіє лише персональними даними, що були зазначені в її резюме, такими

[13] *https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202209596*

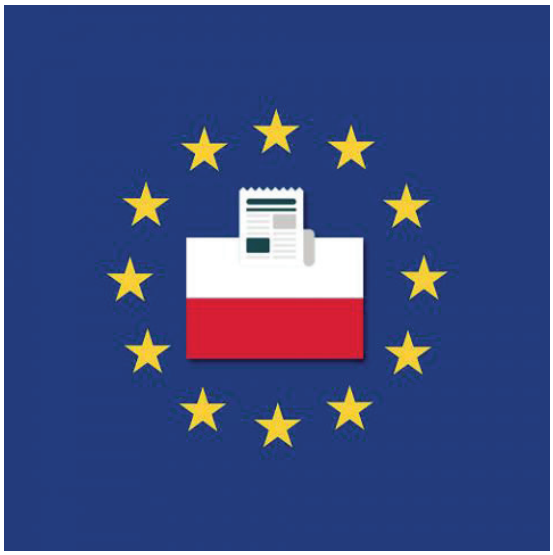
як ідентифікаційні дані, дані про освіту та професійний досвід, і надав їх копію. Контролер також заявив, що він видалив усі персональні дані, пов'язані з суб'єктом даних, включаючи електронні листи та інші повідомлення.

Суб'єкт даних вимагала компенсації, посилаючись на неспроможність контролера належним чином захистити її персональні дані.

Цей інцидент було визнано порушенням згідно зі статтею 5(1)(f) GDPR. У зв'язку з цим AEPD наклало штраф у розмірі 2000 євро, розрахованих на основі річного обороту агентства Blu Management Spain, SL. Відповідно до іспанського закону про адміністративне провадження, AEPD повідомило контролера, що він може визнати свою відповідальність за ймовірні порушення та сплатити запропонований штраф. Кожна з цих дій зменшує накладений штраф на 20%. Контролер вирішив зменшити штраф на 40%, визнавши свою відповідальність за порушення та сплативши зменшену суму штрафу у розмірі - 1200 євро.

13. UODO (Польща)[14]

Наглядовий орган:	UODO (Польща)
Юрисдикція:	Польща
Відповідний закон:	Стаття 5(1)(f) GDPR Стаття 5(2) GDPR Стаття 24(1) GDPR Стаття 25(1) GDPR Стаття 28(1) GDPR Стаття 28(3) GDPR Стаття 32(1) GDPR Стаття 32(2) Стаття 33(3)(c) GDPR Стаття 33(3)(d) GDPR Стаття 34(2) GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	12.11.2024
Штраф:	353 589 злотих



[14] *https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5131.1.2021*

Резюме справи

Фізична особа підприємець — ФОП (контролер) зазнав хакерської атаки внаслідок зараження шкідливим програмним забезпеченням. Зловмисники зашифрували персональні дані клієнтів і співробітників контролера, приблизно 200 осіб. Зашифровані дані складалися, зокрема, з національного ідентифікаційного номера (PESEL), імені та прізвища, адреси, номера поточного рахунку, електронної пошти та номера телефону. Незабаром після атаки контролер відновив доступ до даних. Особи нападників залишилися невідомими.

Контролер зазначив, що порушення сталося через людську помилку. Імовірно, один із співробітників контролера вимкнув антивірусне програмне забезпечення. Крім того, зловмисники також використовували вразливість сервера. Контролер пояснив, що третя сторона, відповідальна за обслуговування сервера (процесор), певний час не оновлювала програмне забезпечення сервера. Це призвело до наявності вразливості під час витоку даних.

Контролер повідомив наглядовий орган з питань захисту персональних даних Польщі (UODO) про витік даних. Завдяки негайному відновленню доступу до даних контролер встановив, що порушення не призвело до високого ризику для прав і свобод суб'єктів даних. Імовірно, єдиною метою зловмисників було отримати викуп від контролера в обмін на доступ до даних, а не отримати доступ до даних і поділитися ними. Спочатку контролер не повідомляв суб'єктів даних відповідно до статті 34 GDPR через технічні та організаційні заходи, вжиті у відповідь на порушення. Зрештою, через місяць після повідомлення наглядового органу, контролер повідомив суб'єктів даних, опублікувавши відповідне оголошення.

Наглядовий орган не знайшло доказів того, що порушення не вплинуло на безпеку даних суб'єктів. Таким чином, наглядовий орган зобов'язав контролера повторно повідомити суб'єктів даних про порушення. Наглядовий орган стверджував, що оригінальне повідомлення було неповним, оскільки в ньому, зокрема, були відсутні контактні дані наглядового органу та опис заходів, застосованих контролером після порушення.

Таким чином, наглядовий орган вирішив порушити провадження проти контролера.

Під час розслідування наглядового органу контролер заявив, що всі співробітники пройшли навчання щодо захисту персональних даних до моменту порушення. Крім того, контролер регулярно створював резервні копії оброблених даних.

Наглядовий орган визнав, що контролер порушив відповідні положення GDPR.

Категорії даних, які обробляє контролер, вимагали підвищеного рівня безпеки. Зокрема, контролер не вжив належних заходів для запобігання зараженню своїх IT-активів шкідливим програмним забезпеченням. Для наглядового органу таким запобіжним заходом є підтримка оновлення програмного забезпечення.

Контролер не оновлював програмне забезпечення сервера приблизно два роки. Більше того, контролер не перевіряв регулярно ризики, які створює його діяльність з обробки даних користувачів. Зокрема, наглядовий орган підкреслив, що контролер не зміг продемонструвати оцінку ризику на захист даних (DPIA), що охоплює потенційну атаку шкідливим програмним забезпеченням.

Наглядовий орган висловив сумнів щодо заходів безпеки, вжитих контролером після порушення. Як зазначав наглядовий орган, не було жодних доказів того, що після порушення було проведено будь-який аудит безпеки IT-активів контролера. У наглядовому органі також відзначили відсутність процедури резервного управління даними. Отже, контролер не зміг відновити доступ до даних без невиправданої затримки.

Таким чином, за інформацією наглядового органу, контролер не проводив оцінку ризиків (DPIA) відповідно до статті 32 GDPR ні до, ні після порушення. Недостатні заходи безпеки призвели до витоку даних і подальшого порушення принципів конфіденційності та цілісності при обробці персональних даних.

Крім того, контролер не перевіряв, як процесор виконував свої обов'язки з безпеки даних. Для наглядового органу таке упущення становило порушення статті 28(1) GDPR. Крім того, контролер не продемонстрував, як процесор допомагав контролеру забезпечити безпеку даних згідно зі статтями 32-36 GDPR. Таким чином, процесор порушив статтю 28(3)(f) GDPR і статтю 32(2) GDPR .

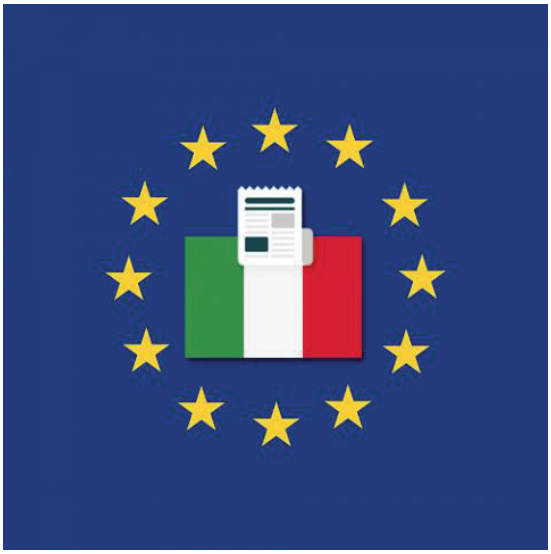
Крім того, контролер порушив статтю 34(2) GDPR . Контролер не надав постраждалим суб'єктам даних достатньо інформації, зокрема про наслідки порушення та доступні засоби захисту.

Як наслідок, наглядовий орган виявив порушення статей 5(1)(f) GDPR , 5(2) GDPR , 24(1) GDPR , 25(1) GDPR , 28(1) GDPR , 28(3) GDPR , 32(1) GDPR , 32(2) GDPR , 33(3) GDPR і 34(2) GDPR.

Контролера оштрафували на 353 589 злотих (приблизно 82 000 євро). Окремо процесор був оштрафований на 9822 злотих (приблизно 2200 євро).

14. Garante per la protezione dei dati personali (Італія)[15]

Наглядовий орган:	Garante per la protezione dei dati personali (Італія)
Юрисдикція:	Італія
Відповідний закон:	Стаття 34(1) GDPR Стаття 34(3)(c) GDPR Стаття 58(2)(e) GDPR
Тип справи:	Розслідування
Дата рішення:	05.11.2024



Резюме справи

Контролер Intesa Sanpaolo (італійський банк) помітив, що співробітник отримав доступ до даних про фінансовий стан 9 суб'єктів даних, хоча ці суб'єкти даних не були клієнтами філії банку.

Співробітник заявив, що вони отримали доступ до даних з професійної зацікавленості. Після внутрішнього аудиту контролер припинив трудові відносини з цим працівником.

17 липня 2024 року контролер повідомив про порушення безпеки даних наглядовий орган відповідно до статті 33 GDPR.

Проте контролер вважає, що порушення даних навряд чи призведе до високого ризику для прав і свобод фізичних осіб. Таким чином, він не повідомив про порушення відповідних суб'єктів даних згідно зі статтею 34(1) GDPR. Однак контролер надіслав неофіційне повідомлення суб'єктам даних, яких це стосується.

Крім того, 10 жовтня 2024 року наглядовому органу стало відомо, що, за даними деяких газет, той самий співробітник здійснив ще 6000 спроб доступу до реквізитів банківських рахунків понад 3500 суб'єктів даних.

Контролер вважав, що порушення не призведе до високого ризику для прав і свобод фізичних осіб. Однак контролер заявив, що може надіслати листа «з турботою про клієнта», щоб пояснити, що сталося.

Незважаючи на те, що розслідування цієї справи все ще відкрито, наглядовий орган визнав за необхідне негайно прийняти рішення щодо необхідності дотримання контролером статті 34 GDPR.

Що стосується статті 34(3)(c) GDPR, наглядовий орган зазначив, що контр-

[15] *https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_%28Italy%29_-_10070521*

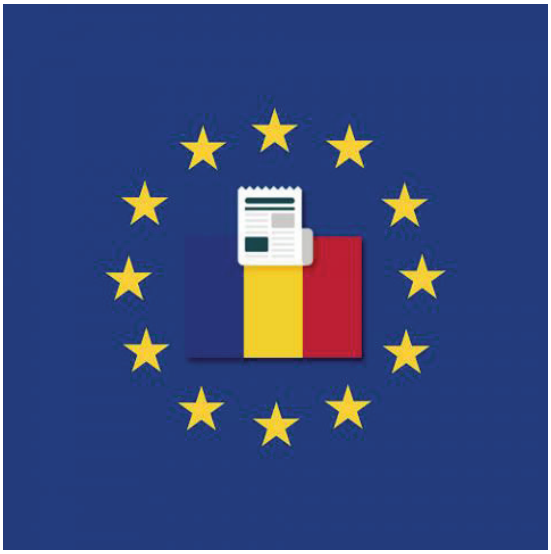
олер, безперечно, має контактні дані суб'єктів даних, оскільки останні є його клієнтами. Тому неможливо стверджувати, що зв'язок із ними потребував би непропорційних зусиль.

Крім того, стосовно листа «з турботою про клієнта», який контролер планує надіслати всім клієнтам, наглядовий орган зазначив, що він має інший зміст і мету, ніж повідомлення, встановлене статтею 34 GDPR.

На цих підставах, згідно зі статтею 34(4) GDPR у поєднанні зі статтею 58(2)(e) GDPR, наглядовий орган зобов'язав контролера повідомити відповідних суб'єктів даних про порушення даних без невиправданої затримки протягом 20 днів. Наглядовий орган наказав, щоб це повідомлення було зроблено особисто працівниками банку, які працюють у відділенні, де було відкрито банківський рахунок відповідних суб'єктів даних.

15. ANSPDCP (Румунія)[16]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 12(3) GDPR Стаття 15(1) GDPR Стаття 15(3) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	04.11.2024
Штраф:	4975,90 лей



Резюме справи

Контролер - компанія, що надає послуги автомобільних перевезень (таксі). Після використання послуг контролера суб'єкт даних подав запит до контролера на доступ до свої персональних даних.

Контролер не відповів протягом терміну, передбаченого статтею 12(3) GDPR. Тому суб'єкт даних подав скаргу до наглядового органу.

У наглядовому органі зазначили, що контролер не відповів на запит суб'єкта даних про доступ до свої персональних даних або, принаймні, не зміг довести, що це зробив.

[16] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_Blackcab_Systems_SRL*

Таким чином, наглядовий орган виявив порушення статті 12(3) GDPR у поєднанні зі статтею 15(1) і 15(3) GDPR.

На цій підставі наглядовий орган наклала штраф на контролера у розмірі 4975,90 лей (1000 євро).

16. Tietosuojavaltuutetun toimisto (Фінляндія)[17]

Наглядовий орган:	Tietosuojavaltuutetun toimisto (Фінляндія)
Юрисдикція:	Фінляндія
Відповідний закон:	Стаття 12(1) GDPR Стаття 15(3) GDPR
Тип справи:	Скарга
Результат:	Відхилено
Дата рішення:	29.10.2024

Резюме справи

Наглядовий орган з питань захисту персональних даних Фінляндії було повідомлено про те, що страхова компанія (контролер) не надала суб'єкту даних усі необхідні документи, електронні листи, записи розмов та інші можливі матеріали, пов'язані з опитуванням про задоволеність клієнтів сервісом компанії. Натомість контролер лише надав стенограму дзвінка, яка, за словами суб'єкта даних, відрізнялася від змісту дзвінка. Потім наглядовий орган попросив контролера пояснити, як він реалізував запит суб'єкта даних.

У відповідь на запит контролер пояснив, що він надав суб'єкту даних всю необхідну інформацію. Контролер пояснив, що, оскільки суб'єкт даних просив надати інформацію поштою, контролер надав суб'єкту даних стенограму дзвінка, яка відображала зміст дзвінка. Потім контролер відправив запис розмови та інші документи суб'єкту даних поштою на флеш-накопичувачі.

Суб'єкт даних звернувся до наглядового органу з проханням вирішити, чи відповідає розшифровка запису розмови достовірності розмови та чи мав контролер надати копію запису розмови поштою негайно чи лише після нового запиту суб'єкта даних.

[17] *https://gdprhub.eu/index.php?title=Tietosuojavaltuutetun_toimisto_(Finland)_-_TSV/428/2022*

На основі інформації, наданої контролером, наглядовий орган вважає, що контролер повинен оцінити в кожному конкретному випадку відповідний формат, у якому надавати персональні дані, запитувані відповідно до статті 15 GDPR . Наглядовий орган підкреслив, що персональні дані не завжди потрібно надавати в оригінальному форматі, якщо дані можуть бути належним чином надані в іншій формі.

У наглядовому органі зазначили, що інформація, надана контролером, дозволила особі перевірити достовірність персональних даних. Таким чином, наглядовий орган вважає, що контролер виконав вимоги статті 12(1) GDPR та статті 15(3) GDPR , спочатку надавши письмову стенограму запису розмови.

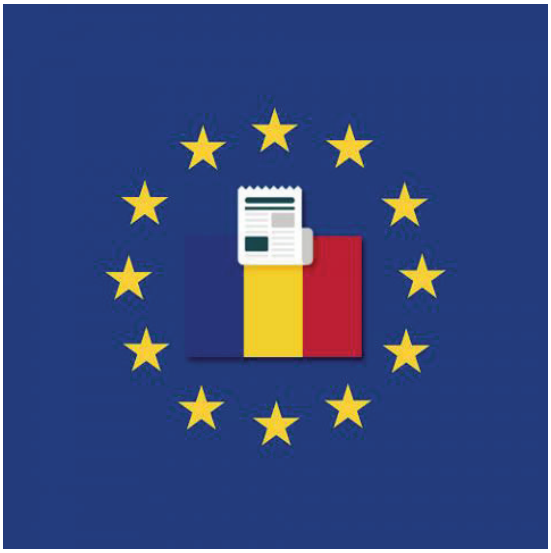
Що стосується вмісту запису розмови, наглядовий орган виявив, що транскрипція розмови відповідає змісту розмови з точністю, яку дозволяв характер запису розмови. Наглядовий орган встановив, що ключовим фактором у цій справі було те, що суб'єкту даних також була надана копія запису розмови в електронній формі, що дозволило суб'єкту даних оцінити як зміст транскрипції, так і зміст розмови - запис.

На підставі зібраної інформації наглядовий орган дійшов висновку, що контролер надав суб'єкту даних всю необхідну інформацію, а тому повністю задовольнив запит на доступ.

У результаті наглядовий орган постановив, що контролер виконав вимоги статті 12(1) GDPR та статті 15(3) GDPR, виконавши запит суб'єкта даних на доступ до даних, спочатку надавши письмову розшифровану версію запису розмови.

17. ANSPDCP (Румунія)[18]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 6(1)(a) GDPR Стаття 7(1) GDPR Стаття 12(1) GDPR Стаття 21(2) GDPR Стаття 21(3) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	25.10.2024
Штраф:	9951,40 лей



Резюме справи

Контролер керує веб-сайтом, на якому продаються квитки на концерти.

Щоб використовувати цю платформу, суб'єкт даних створив обліковий запис і ввів свій номер телефону. Після цього суб'єкт даних отримав на свій телефон декілька текстових повідомлень з рекламою послуг контролера.

Суб'єкт даних заперечив проти обробки свого номера телефону для цілей прямого маркетингу відповідно до статті 21(2) GDPR.

Після цього контролер повністю видалив його обліковий запис і відмовився його повторно активувати.

Таким чином, суб'єкт даних подав скаргу до наглядового органу.

Наглядовий орган постановив, що контролер відреагував незаконно, отримавши заперечення суб'єкта даних, оскільки він повністю дезактивував і видалив профіль суб'єкта даних.

Таким чином, наглядовий орган виявив порушення статті 12(1) GDPR у поєднанні зі статтею 21(2) і 21(3) GDPR.

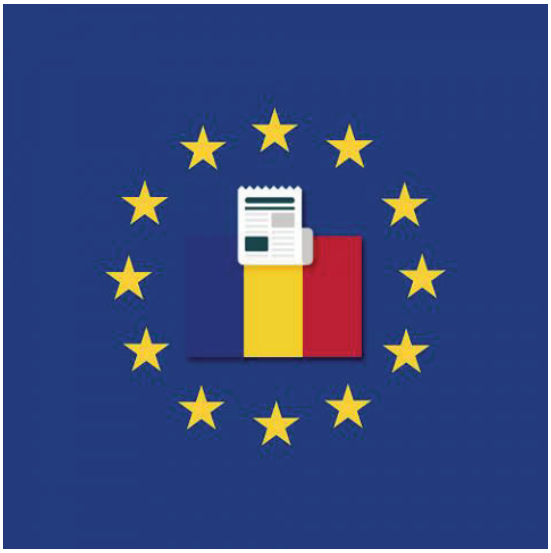
Крім того, наглядовий орган зазначив, що контролер ніколи не отримував згоду суб'єкта даних перед тим, як надсилати йому SMS повідомлення для цілей прямого маркетингу. Тому було встановлено порушення статей 6(1)(a) і 7(1) GDPR.

На цій підставі наглядовий орган наклав штраф на контролера у розмірі 9951,40 лей (2000 євро).

[18] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_IA_BILET_SRL*

18. ANSPDCP (Румунія)[19]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 25(1) GDPR Стаття 32(1)(a) GDPR Стаття 32(1)(b) GDPR Стаття 32(1)(d) GDPR Стаття 32(2) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	16.10.2024
Штраф:	14 929,20 лей



Резюме справи

У період з березня по квітень 2024 року третя сторона мала авторизований доступ до персональних даних, що зберігаються на сервері контролера.

Зокрема, порушення стосувалося імені та прізвищ суб'єктів даних, їх персонального ідентифікаційного номера та кількості путівок на відпочинок, які вони отримали.

Суб'єкт даних подав скаргу до наглядового органу.

По-перше, наглядовий орган зазначив, що це порушення сталося через те, що контролер не вжив належних технічних та організаційних заходів для забезпечення безпеки обробки. Це призвело до несанкціонованого доступу до цих даних.

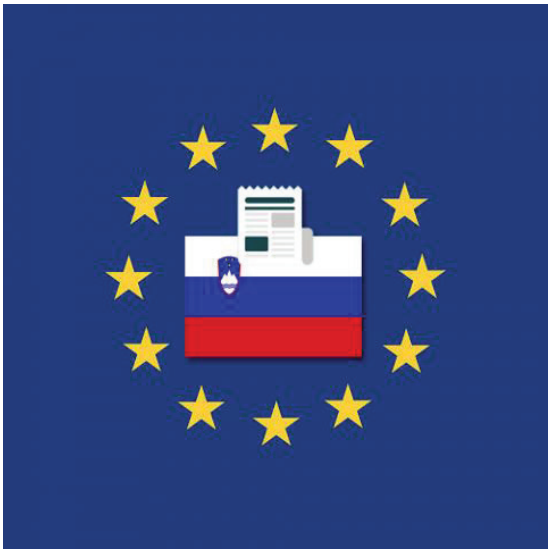
Таким чином, наглядовий орган виявив порушення статей 25(1), 32(1)(a) , 32(1)(b) , 32(1)(d) і 32(2) GDPR і наклав штраф у розмірі 14 929, 20 лей (3000 євро).

Крім того, згідно зі статтею 58(2) GDPR наглядовий орган наказав контролеру запровадити механізм для регулярного тестування та оцінки ефективності вжитих заходів, беручи до уваги ризик, пов'язаний з обробкою, з метою забезпечення належного рівня безпеки даних, щоб уникнути подібних інцидентів порушення безпеки в майбутньому.

[19] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_Your_Consulting_SRL*

19. IP (Словенія)[20]

Наглядовий орган:	IP (Словенія)
Юрисдикція:	Словенія
Відповідний закон:	Стаття 5(1)(a) GDPR Стаття 6(1) GDPR Стаття 13(1) GDPR Стаття 83(5)(a) GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	16.10.2024
Штраф:	25 000 євро



Резюме справи

У невстановлену дату в минулому контролер встановив відеокамери на території свого підприємства. Деякі камери були спрямовані прямо на робочі місця співробітників. Камери знімали співробітників на роботі, і ці записи були доступні контролеру (керівник) через мобільний телефон, а також через веб-сайт.

Суб'єкти даних не мали доступу до записів. На вході на робоче місце не було чітко видно повідомлення про ведення відеозйомки. Контролер розмістив повідомлення про ведення відеозйомки всередині приміщення в невідомому місці.

Повідомлення про відеозйомку не містило інформації про правові наслідки ведення відеозйомки, контактні дані контролера, чи була інформація передана третім особам, а також будь-яку інформацію, необхідну згідно зі статтею 13(1) GDPR . Крім того, в повідомленні не було жодного посилання на веб-сайт, де можна було б знайти цю інформацію.

Відтак наглядовий орган розпочав розслідування у цій справі. Інформаційний уповноважений Республіки Словенія притягнув до відповідальності керівника компанії як контролера, а також компанію в цілому в особі контролера. Наглядовий орган постановив, що контролер порушив статтю 76(4) Закону Республіки Словенія «Про захист персональних даних». Ця стаття чітко визначає вимоги, які має містити повідомлення про інформування суб'єктів даних про відеоспостереження, наприклад, цілі обробки,

[20] *https://gdprhub.eu/index.php?title=IP_(Slovenia)_-_0603_30_2023_12*

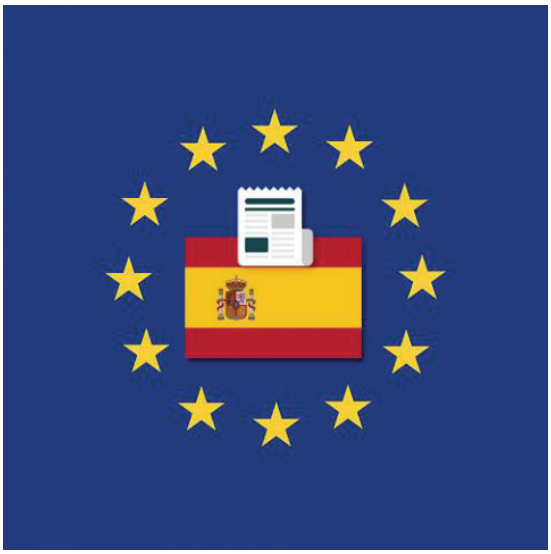
номер телефону або адресу електронної пошти чи веб-адресу для цілей реалізації прав особи у сфері захисту персональних даних.

Усі ці вимоги контролером не були дотримані, а далі наглядовий орган встановив, що єдиною метою відеозйомки було просто стеження за працівниками. Він заявив, що якби запис проводився з законною метою, як-от забезпечення безпеки приміщень, співробітників і бізнесу, достатньо було б розміщення камер виключно для цих цілей. В наглядовому органі пояснюють, що камер на вході в будівлю та на касах було б цілком достатньо. Наглядовий орган стверджував, що просте спостереження за працівниками не є законною підставою для обробки.

Передачу даних на загальнодоступний веб-сайт було визнано порушенням статті 5(1)(a) і статті 6(1) GDPR, оскільки для цього не було законної підстави. Компанію оштрафували на 25 000 євро, а керівника — 1750 євро.

20. AEPD (Іспанія)[21]

Наглядовий орган:	AEPD (Іспанія)
Юрисдикція:	Іспанія
Відповідний закон:	Стаття 6(1) GDPR Стаття 83(5) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	16.10.2024
Штраф:	60 000 євро



Резюме справи

13 квітня 2023 року суб'єкт даних подав скаргу до Іспанського агентства із захисту персональних даних (AEPD) на контролера - постачальника електроенергії. Суб'єкт даних був клієнтом контролера до 2021 року та 12 квітня 2022 року знову хотів зареєструватися як клієнт у контролера. Команда контролера з обслуговування клієнтів зв'язалася з суб'єктом даних, щоб підтвердити його обліковий запис і номер телефону.

Суб'єкт даних стверджував, що контролер все ще володіє персональними даними суб'єкта даних, такими як

[21] *https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202307313*

номер його ідентифікаційної картки, його ім'я та адреса, оскільки йому не потрібно було надавати ці дані заново.

Після надання даних команді контролера з обслуговування клієнтів суб'єкт даних отримав електронний лист від контролера, а також від іншої електроенергетичної компанії, компанії-партнера контролера, з проханням підписати додатковий договір у форматі PDF. Договір містив персональні дані, такі як ім'я, адреса та IBAN суб'єкта даних. Таким чином, суб'єкт даних дійшов висновку, що контролер передав персональні дані своїй партнерській компанії без згоди суб'єкта даних.

Після подання скарги AEPD розпочало розслідування для з'ясування обставин справи. Компанія-партнер повідомила AEPD, що контролер і вона не підтримують будь-які відносини в обробці персональних даних і що кожна компанія обробляє дані виключно своїх власних клієнтів. Однак обидві компанії належать іспанській багатонаціональній електроенергетичній компанії Iberdrola. Компанія-партнер переконалася, що існує система, яка визначає, які клієнти до якої компанії належать. Компанія-партнер також стверджувала, що працівник служби підтримки клієнтів припустився помилки та надіслав договір не від тієї компанії.

Контролер також зазначив, що лише через три години вони відповіли на електронний лист суб'єктів даних із повідомленням про помилку з вибаченнями.

31 липня 2024 року AEPD розпочало провадження щодо контролера. Він підкреслив, що контролер безвідповідально поводився з даними, що призвело до того, що інший суб'єкт отримав доступ до даних без згоди суб'єкта даних. AEPD підтвердило, що передача даних компанії-партнеру була обробкою, на яку суб'єкт даних ніколи не давав згоди.

AEPD постановило, що контролер порушив статтю 6(1) GDPR , і призначив штраф у розмірі 100 000 євро на основі річного обороту контролера (стаття 83(5) GDPR). Штраф було зменшено до 60 000 євро, оскільки контролер погодився з рішенням наглядового органу та процедурою добровільної оплати.

21. HDPA (Греція)[22]

Наглядовий орган:	HDPA (Греція)
Юрисдикція:	Греція
Відповідний закон:	Стаття 5(1)(a) GDPR Стаття 6(1) GDPR Стаття 6(4) GDPR Стаття 9(1) GDPR Стаття 9(2) GDPR Стаття 12(2) GDPR Стаття 13 GDPR Стаття 14 GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	11.10.2024
Штраф:	15 000 євро

Резюме справи

4 травня 2023 року суб'єкт даних отримала небажане SMS повідомлення від контролера, якого вона не знала особисто. Під час розслідування вона виявила через Facebook, що контролер працював лікарем в лікарні, яку вона часто відвідувала. Повідомлення мало політичний зміст. Подібну скаргу наступного дня подав інший суб'єкт даних.

Наглядовий орган з захисту персональних даних Греції ініціював розслідування, зв'язавшись із лікарнею, щоб отримати інформацію з цього приводу.

У своїй відповіді контролер висунув наступні аргументи:

1. Телефонні номери або належали особам у його особистій мережі контактів, або були згенеровані за допомогою генератора випадкових чисел.

2. Повідомлення не стосувалися інформації про стан здоров'я одержувачів.

3. Після відправки повідомлень він завантажив форму згоди та повідомлення про конфіденційність на свою сторінку у Facebook.

[22] *https://gdprhub.eu/index.php?title=HDPA_(Greece)_-_37/2024*

4. Він посилався на легітимний інтерес згідно зі статтею 6(1)(f) GDPR як правову підставу для обробки даних для повідомлення про свою політичну діяльність.

5. Він заперечував використання даних пацієнтів з лікарняних справ для своєї політичної кампанії.

Наглядовий орган запросив детальні роз'яснення від контролера, зокрема загальну кількість одержувачів SMS, походження їхніх телефонних номерів, частоту використання форми згоди, точний графік публікації повідомлення про конфіденційність та заходи, вжиті з метою забезпечення прав одержувачів (суб'єктів даних) відповідно до GDPR.

Контролер повідомив, що 4772 особи отримали SMS, стверджуючи, що 75% були з його особистої мережі контактів. Він також стверджував, що суб'єкти даних можуть реалізувати свої права відповідно до GDPR через його сторінку у Facebook.

Для порівняння наглядовий орган отримав список телефонів пацієнтів із лікарні. Серед 4772 одержувачів повідомлень 3392 номери збігалися зі списком лікарні. Крім того, обидва списки містили 17 телефонних номерів з однаковими помилками. Пізніше контролер переглянув свої попередні показання, що використовував для розсилки дані зі своєї особистої мережі контактів. Наглядовий орган запросив додаткові роз'яснення та запросив контролера на ще одне усне слухання.

Наглядовий орган, заслухавши контролера, лікарню та суб'єктів даних, постановив, що контролер порушив (статтю 5(1)(a) GDPR , статтю 6(1) GDPR та статтю 6(4) GDPR. Крім того, він не сприяв реалізації прав суб'єктів даних відповідно до GDPR, наприклад, відповідно до статті 13 GDPR та статті 14 GDPR. Висновки наглядового органу базувалися на таких аргументах:

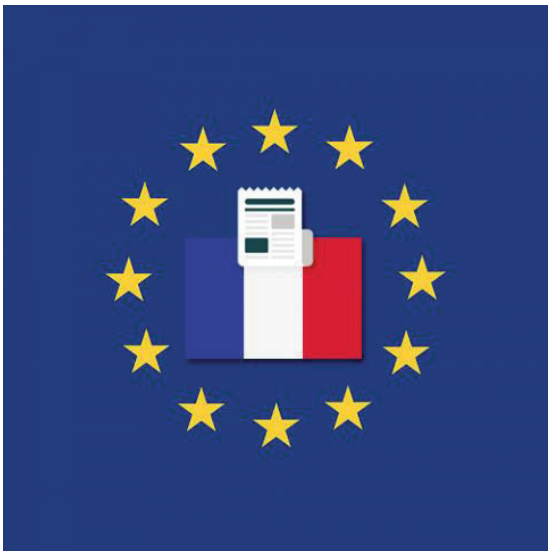
1. Контролер постійно змінював свої пояснення у відповідь на докази, надані наглядовим органом, підриваючи довіру до нього.

2. Він не зміг достовірно визначити джерела використаних телефонних номерів, що робить неправдоподібним те, що така значна частина контактних даних його пацієнтів була включена випадково або згенерована випадковим чином.

З огляду на серйозність порушення , рівень відповідальності контролера, який є лікарем, у поєднанні з його зобов'язанням щодо конфіденційності та, нарешті, суперечливі аргументи, представлені під час слухань, наглядовий орган вирішив накласти на контролера штраф у розмірі 15 000 євро.

22. CNIL (Франція)[23]

Наглядовий орган:	CNIL (Франція)
Юрисдикція:	Франція
Відповідний закон:	Стаття 5(1)(e) GDPR Стаття 9 GDPR Стаття L34-5 Кодексу електронних комунікацій Республіки Франція
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	10.10.2024
Штраф:	150 000 євро



Резюме справи

Контролер надавав дистанційні послуги психолога/астролога за допомогою телефону, онлайн-чату чи SMS повідомлень. На деяких своїх веб-сайтах контролер пропонував персоналізовані чати по телефону, які проводив його партнер. Щоб просувати свої послуги, дві компанії надсилали маркетингові повідомлення існуючим і потенційним клієнтам електронною поштою та текстовими SMS повідомленнями. Контактні дані потенційних клієнтів були отримані за допомогою контактної форми на веб-сайтах обох компаній. Контролер та його партнер створили спільну базу даних для своїх маркетингових цілей, яка станом на 6 жовтня 2022 року включала персональні дані понад 1,5 мільйона людей.

15 листопада 2021 року Національна комісія у справах інформаційних технологій і прав людини (CNIL) провела перевірку п'яти веб-сайтів, якими керує контролер та його партнер. Також 7 та 8 грудня 2021 року на території двох компаній було проведено виїзну перевірку.

Висновки розслідування:

1) Стаття 5(1)(e) GDPR

Контролер зберігав дані своїх клієнтів протягом шести років після закінчення комерційних відносин. Контролер стверджував, що це необхідно для того, щоб мати можливість реагувати на можливі судові розслідування.

[23] *https://gdprhub.eu/index.php?title=CNIL_(France)_-_SAN-2024-015*

2) Стаття 9 GDPR

Контролер пропонує користувачам свого веб-сайту horoscope.fr заповнити форму, призначену для надання безкоштовного прогнозу щодо їх романтичної сумісності з обраною особою. Користувачі повинні ввести свою стать, дату, час і місто народження, а також адресу електронної пошти, а також стать і дату народження свого партнера. Під час дистанційних консультацій клієнти можуть розкрити велику кількість особистої інформації. Ці розмови записуються партнером контролера, і половина даних зберігається до кінця робочого дня, а друга половина зберігається протягом шести місяців.

Контролер стверджував, що ці конфіденційні дані не обробляються, а просто записуються.

3) Обробка персональних даних в маркетингових цілях згідно зі статтею L34-5 Кодексу електронних комунікацій Республіки Франція

У сповіщенні, включеному в контактну форму, не вказано ні контролера, ні списку всіх інших третіх сторін, яким надаються дані. Хоча користувачі могли перейти за посиланням, яке надавало додаткову інформацію, це посилання було розташоване набагато нижче у формі. Крім того, в інформації, включеній у посилання, взагалі не згадується комерційна реклама.

Під час розслідування контролер змінив формат контактної форми, включивши дуже маленький незрозумілий символ до слова у формі. Натискання на цей символ призводить до виноски, яка не була видима в оригінальній формі, в якій зазначено контролера як постачальника маркетингових повідомлень.

Контролер стверджував, що було б неможливо надати суб'єктам даних вичерпний список одержувачів, оскільки це порушило б договірні положення про конфіденційність.

Таким чином:

1) Стаття 5(1)(e) GDPR

CNIL уточнює, що контролер не зіткнеться з жодними санкціями, якщо він видалить персональні дані клієнтів, оскільки більше не потрібно обробляти їх для визначених контролером цілей. Таким чином, CNIL не прийняв аргумент контролера щодо гарантування шестирічної політики зберігання.

Оскільки дані збираються для певної мети, якою є управління комерційними відносинами, CNIL заявляє, що як тільки мета обробки змінюється, контролер повинен вжити заходів для диференціації даних. Таким чином, практика однозначного збирання всіх даних клієнтів в активну базу даних без будь-якої диференціації чи архівування є порушенням статті 5(1)(e) GDPR. Що стосується управління комерційними відносинами, CNIL рекомендує максимальний період зберігання три роки після закінчення комерційних відносин.

2) Стаття 9 GDPR

CNIL зазначає, що запис розмови, збереження і видалення даних підпадає під визначення обробки згідно зі статтею 4(2) GDPR, тому відхиляє аргумент контролера. Всупереч положенням статті 4(11) GDPR, CNIL зазначає, що компанія не надає жодної конкрет-

ної інформації суб'єктам даних щодо збору та обробки даних, зібраних із форми на веб-сайті, і не збирає їх однозначно вираженої згоди на обробку таких даних. Подібним чином у контексті чату чи текстових консультацій не надається інформація про обробку таких даних або отримана згода, як того вимагає стаття 9(2)(a) GDPR.

Тому CNIL робить висновок про порушення статті 9 GDPR , оскільки просте бажання ввести інформацію у форму або поділитися особистою інформацією через параметри чату не дорівнює повністю інформованій згоді на обробку цих даних.

3) Обробка персональних даних в маркетингових цілях згідно зі статтею L34-5 Кодексу електронних комунікацій Республіки Франція

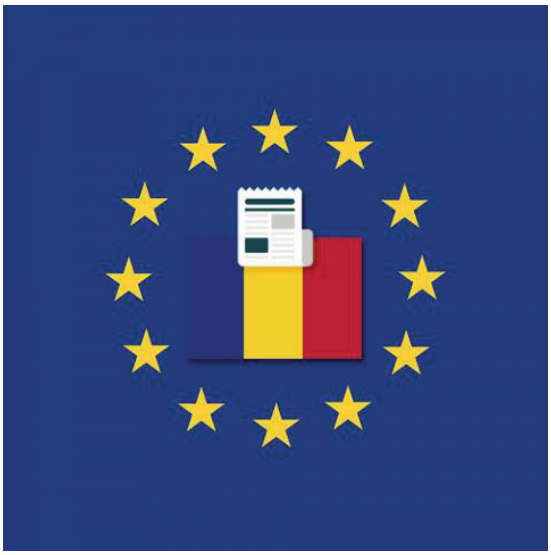
CNIL заявив, що вдосконалення, внесені до форми, все ще не відповідають необхідному стандарту, який дозволяє суб'єкту даних легко отримати доступ до чіткого опису маркетингових цілей і партнерів, як того вимагає французьке законодавство.

4) Висновок

CNIL дійшов висновку, що контролер порушив статтю 5(1)(e) GDPR , статтю 9 GDPR і статтю L34-5 Кодексу електронних комунікацій Республіки Франція. З огляду на річний оборот контролера, було встановлено штраф у розмірі 100 000 євро за порушення статті 5(1)(e) GDPR , статті 9 GDPR і штраф у розмірі 50 000 євро за порушення статті L34-5 Кодексу електронних комунікацій Республіки Франція.

23. ANSPDCP (Румунія)[24]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 5(1)(c) GDPR Стаття 5(1)(e) GDPR Стаття 5(1)(a) GDPR Стаття 5(2) GDPR Стаття 6(1) GDPR Стаття 12 GDPR Стаття 14 GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	02.10.2024
Штраф:	9947,60 лей



Резюме справи

Контролер встановив на службовому автомобілі систему GPS-моніторингу. За словами контролера, метою цього була необхідність ведення обліку робочого часу працівників. Суб'єкти даних не були проінформовані про існування такого пристрою стеження.

Суб'єкт даних (працівник) подав скаргу до наглядового органу з питань захисту персональних даних Румунії.

По-перше, наглядовий орган виявив, що така діяльність з обробки даних контролером здійснюється з порушенням статей 5(1)(a) , 5(1)(c) , 5(2) і 6 GDPR.

По-друге, наглядовий орган зазначив, що контролер не надав суб'єкту даних інформацію, визначену статтею 14 GDPR. Тому він виявив порушення цієї статті в поєднанні зі статтею 12 GDPR.

Нарешті, наглядовий орган зазначив, що контролер зберігав дані протягом 6 місяців, що перевищує період у 30 днів, встановлений статтею 5(1)(e) Закону Румунії «Про захист персональних даних». Тому він виявив порушення статті 5(1)(e) GDPR.

На цій підставі він оштрафував контролера на 9947,60 лей (2000 євро).

[24] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_Global_Ports%E2%80%99s_Services_S.R.L.*

24. Tietosuojavaltuutetun toimisto (Фінляндія)[25]

Наглядовий орган:	Tietosuojavaltuutetun toimisto (Фінляндія)
Юрисдикція:	Фінляндія
Відповідний закон:	Стаття 12(2) GDPR Стаття 15 GDPR Стаття 15(3) GDPR Стаття 58(2)(b) GDPR Стаття 58(2)(d) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	27.09.2024

Резюме справи

Наглядовий орган з питань захисту персональних даних Фінляндії було повідомлено, що податкова адміністрація Фінляндії (контролер) висунула необґрунтовані вимоги для виконання запиту на доступ і відмовилася надати копію персональних даних суб'єкта даних його представнику. Суб'єкт даних, який проживав за кордоном, звернувся до контролера з проханням надати персональні дані за допомогою електронної пошти або на поштову адресу свого представника в Фінляндії.

У відповідь на запит контролер пояснив, що він може надати персональні дані лише безпосередньо суб'єкту даних, оскільки право доступу згідно зі статтею 15 GDPR є особистим правом і вимагає персонального запиту суб'єкта даних.

Контролер також заявив, що не може надати копію персональних даних суб'єкта даних електронною поштою. Натомість контролер запропонував суб'єкту даних переглядати свої персональні дані, увійшовши в захищений сервіс контролера MyTax. Крім того, запит на доступ можна зробити в письмовій формі, надіславши власноруч підписану форму запиту на доступ, і в цьому випадку контролер надасть персональні дані суб'єкту даних поштою.

На підставі інформації, наданої контролером, наглядовий орган вважав, що запит суб'єкта даних не міг бути належним чином виконаний шляхом на-

[25] *https://gdprhub.eu/index.php?title=Tietosuojavaltuutetun_toimisto_(Finland)_-_TSV/91/2020*

правління суб'єкта даних переглянути свої персональні дані в онлайн-сервісі контролера.

У наглядовому органі зазначили, що контролер не може вимагати від суб'єкта даних підписання запиту на доступ або подання його поштою. Такі вимоги не сприяють здійсненню прав суб'єктів даних, як того вимагає стаття 12(2) GDPR, а, навпаки, роблять надсилання запиту на доступ надмірно обтяжливим. У наглядовому органі підкреслили, що GDPR не висуває жодних формальних вимог до запитів щодо реалізації прав суб'єктів даних.

Наглядовий орган виявив, що GDPR не забороняє використовувати представника, наприклад, для отримання копій документів, пов'язаних із запитом на доступ. Таким чином, контролер не повинен був відхилити запит суб'єкта даних лише на цій підставі.

На основі зібраної інформації наглядовий орган постановив, що контролер порушив статтю 12(2) GDPR.

У результаті наглядовий орган оголосив контролеру догану відповідно до статті 58(2)(b) GDPR . Згідно зі статтею 58(2)(d) GDPR, наглядовий орган також наказав контролеру привести свої операції з обробки даних у відповідність до GDPR щодо обробки запитів на доступ, включаючи можливість використання представника.

25. ICO (Великобританія)[26]

Наглядовий орган:	ICO (Великобританія)
Юрисдикція:	Велика Британія
Відповідний закон:	58(2)(b) UK GDPR 6(1)(a) UK GDPR 7(1) UK GDPR Стаття 5(1)(a) UK GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	17.09.2024

[26] *https://gdprhub.eu/index.php?title=ICO_(UK)_-_Bonne_Terre_Ltd_and_Sky_Betting_and_Gaming*

Резюме справи

Контролер, постачальник послуг онлайн-ігор і ставок, використовував сторонню технологію відстеження, включаючи файли cookie, для збору персональних даних у маркетингових цілях. Після звіту правозахисної організації про те, що контролер передає великі обсяги даних третім особам без згоди суб'єктів даних, Офіс інформаційного комісара (ICO) Великої Британії розпочав розслідування.

Було виявлено, що коли користувачі відвідували веб-сайт, вони повинні були дати згоду на файли cookie. Однак ще до того, як згода була надана шляхом вибору в банері cookie відповідного налаштування, файли cookie розміщувалися на пристроях відвідувачів. Просте відвідування веб-сайту ініціювало обробку персональних даних, які були передані третім особам без відома або згоди користувачів.

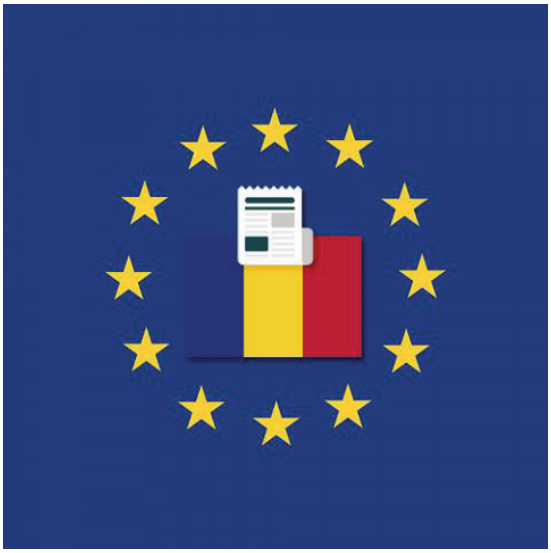
2 березня 2023 року ICO попередив контролера про свою невідповідну практику, і наступного дня контролер вжив заходів для вирішення проблеми. Виправлення проблеми було підтверджено ICO через форму технічного тестування 17 березня 2023 року.

17 березня 2023 року контролер заявив, що вся обробка персональних даних відбувалася відповідно до правової підстави - згоди. Таким чином, ICO дійшов висновку, що з 10 січня 2023 року до 3 березня 2023 року обробка відбувалася незаконно. Деякі файли cookie були розгорнуті без відома або згоди користувачів до того, як вони взаємодіяли з банером cookie.

Заявивши, що незаконне розкриття персональних даних третім особам викликає значне занепокоєння громадськості. Таким чином ICO визнав обробку незаконною. ICO оголосив контролеру догану відповідно до статті 58(2)(b) UK GDPR за порушення статей 5(1)(a), 6(1)(a) і 7(1) UK GDPR.

26. ANSPDCP (Румунія)[27]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 32(1) GDPR Стаття 32(2) GDPR Стаття 33 GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	17.09.2024
Штраф:	14 929,50 лей



Резюме справи

Контролер зазнав порушення безпеки персональних даних своїх працівників у Румунії (ім'я/прізвище, дата народження, адреси, номери домашніх телефонів та особиста електронна пошта). Неавторизована третя сторона отримала доступ до цих даних.

Контролер повідомив про це порушення даних наглядовому органу відповідно до статті 33 GDPR.

Наглядовий орган постановив, що контролер не вжив належних технічних та організаційних заходів для забезпечення належного рівня безпеки, відповідного ризиків обробки.

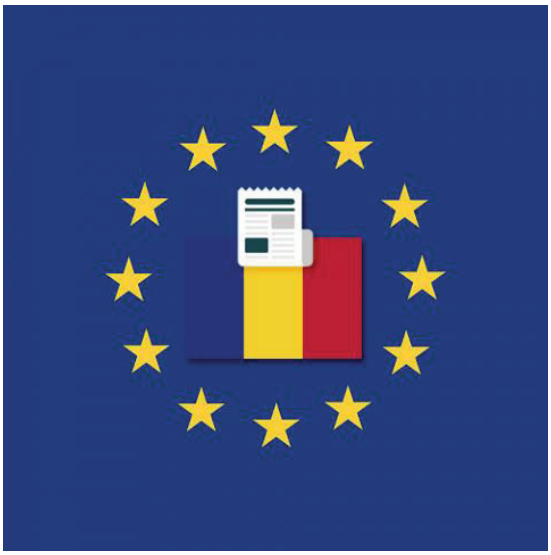
Тому він виявив порушення статті 32(1) і 32(2) GDPR.

На цій підставі він наклав штраф у розмірі 14 929,50 лей (3 000 євро) і зобов'язав контролера переглянути та оновити свої технічні та організаційні заходи щодо безпеки персональних даних, які обробляються через його IT-інфраструктуру.

[27] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_Constan%C8%9Ba_South_Container_Terminal_SRL*

27. ANSPDCP (Румунія)[28]

Наглядовий орган:	ANSPDCP (Румунія)
Юрисдикція:	Румунія
Відповідний закон:	Стаття 12(3) GDPR Стаття 15 GDPR Стаття 17 GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	16.09.2024
Штраф:	14 930 лей



Резюме справи

Суб'єкт даних надіслав контролеру (оператор мобільного зв'язку) запит на доступ до даних і запит на видалення даних.

Контролер не відповів суб'єкту даних протягом терміну, встановленого статтею 12(3) GDPR.

Тому суб'єкт даних подав скаргу до наглядового органу. Лише після того, як наглядовий орган розпочав розслідування щодо контролера, останній розпочав розгляд запитів суб'єкта даних.

Наглядовий орган зазначив, що контролер не зміг виконати запит суб'єкта даних на доступ і видалення без невиправданої затримки та, в будь-якому випадку, протягом одного місяця з моменту запиту.

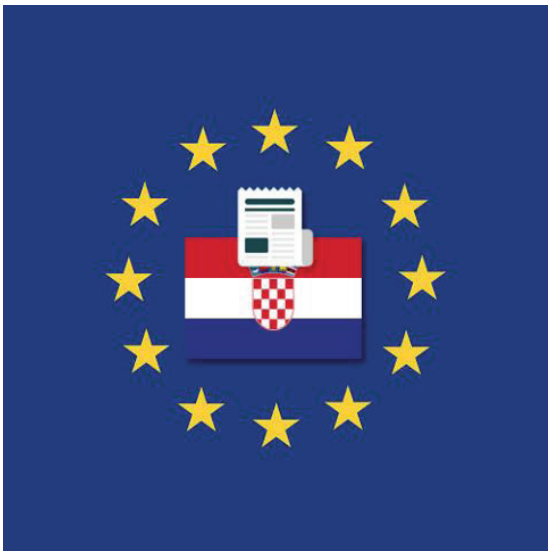
Тому він виявив порушення статті 12(3) GDPR у поєднанні зі статтями 15 і 17 GDPR.

На цій підставі він наклав штраф на контролера у розмірі 14 930 лей (3 000 євро) і зобов'язав контролера прийняти внутрішню процедуру щодо того, як розглядати запити, подані суб'єктами даних відповідно до GDPR у встановлені законом терміни.

[28] *https://gdprhub.eu/index.php?title=ANSPDCP_(Romania)_-_Fine_against_Vodafone_Romania_SA*

28. AZOP (Хорватія)[29]

Наглядовий орган:	AZOP (Хорватія)
Юрисдикція:	Хорватія
Відповідний закон:	Стаття 5(2) GDPR Стаття 6(1) GDPR Стаття 13 GDPR Стаття 28(3) GDPR Стаття 32(1)(b) GDPR Стаття 33(1) GDPR Стаття 38(1) GDPR
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	13.09.2024
Штраф:	190 000 євро



Резюме справи

У липні 2019 року контролер (лікарня), зазнав порушення безпеки даних у радіологічній інформаційній системі. Це призвело до втрати зображень рентгенівських досліджень, які зберігалися в радіологічній інформаційній системі лікарні. Контролер не повідомив наглядовий орган про це порушення безпеки даних.

У вересні 2022 року кілька суб'єктів даних подали запити на доступ, вимагаючи копії своїх медичних зображень. Оскільки контролер не зміг надати їм ці копії, вони подали скаргу до наглядового органу.

Також з'ясувалося, що контролер записував телефонні розмови через кол-центр, не повідомляючи суб'єктів даних.

Контролер стверджував, що він не знав про витік даних до 2022 року і що він не вжив жодних заходів для забезпечення безпеки даних про здоров'я, оскільки це потребувало б більших ресурсів та інвестицій в інформаційну систему лікарні.

Розслідування:

По-перше, наглядовий орган зазначив, що його не було повідомлено про

[29] *https://gdprhub.eu/index.php?title=AZOP_(Croatia)_-_Decision_13-09-2024*

порушення безпеки даних протягом терміну, встановленого статтею 33(1) GDPR . Він зазначив, що контролеру не можна вірити, коли він стверджує, що дізнався про витік даних у 2022 році. Навпаки, наглядовий орган знайшов докази того, що головний радіолог помітив витік даних і повідомив про це керівництво контролера в липні 2019 року. Таким чином, наглядовий орган виявив порушення статті 33(1) GDPR.

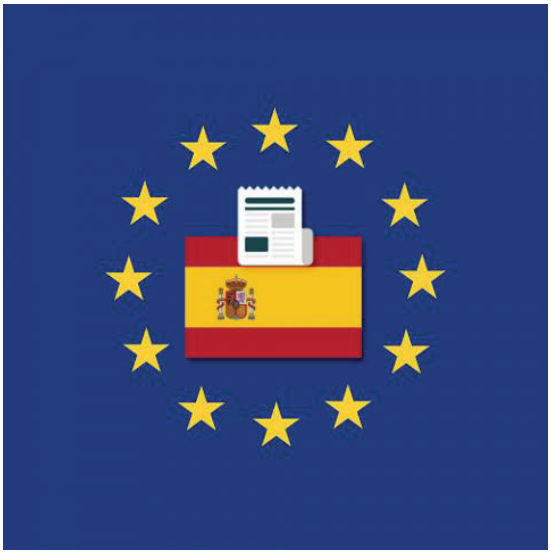
По-друге, наглядовий орган звернув увагу на те, що контролер не запровадив відповідних технічних заходів безпеки даних, які бути втрачені, тобто не створив резервну копію даних. Ця помилка призвела до безповоротної втрати персональних даних. Таким чином, наглядовий орган виявив порушення статті 32(1)(b) GDPR.

По-третє, наглядовий орган виявив, що зовнішня компанія (процесор) відповідала за впровадження та підтримку IT-системи. Однак контролер і цей процесор не уклали угоду про обробку даних і, таким чином, порушили статтю 28(3) GDPR.

На цій підставі наглядовий орган наклала штраф на контролера у розмірі 190 000 євро.

29. APDCAT (Каталонія)[30]

Наглядовий орган:	APDCAT (Каталонія)
Юрисдикція:	Іспанія
Відповідний закон:	Стаття 5(1)(a) GDPR Стаття 9(2)(b) GDPR Стаття 35(1) GDPR Стаття 35(3)(b) GDPR Стаття 35(4) GDPR Стаття 28(2) LOPDGDD
Тип справи:	Скарга
Результат:	Виявлено порушення
Дата рішення:	10.09.2024



[30] *https://gdprhub.eu/index.php?title=APDCAT_(Catalonia)_-_PS_33/2024*

Резюме справи

1 січня 2021 року контролер (муніципалітет), запровадив нову систему обліку часу для своїх працівників. Ця система призвела до того, що працівники повинні були використовувати відбитки пальців для обліку свого робочого часу.

13 січня 2024 року деякі суб'єкти даних подали скаргу до наглядового органу.

Контролер стверджував, що правовою підставою для обробки, на яку він може посилатися, є стаття 6(1)(c) GDPR.

Крім того, було зазначено, що система не фіксує біометричні дані, а лише деякі характерні ознаки для того, щоб мати можливість автентифікувати користувачів. Також, було зазначено, що в будь-якому випадку відбиток пальця використовувався як унікальний ідентифікатор, який можна відтворити в інших системах.

Нарешті, він стверджував, що оцінка впливу на конфіденційність (DPIA) не була потрібна, оскільки не передбачалося обробки будь-яких конфіденційних даних.

Розслідування:

По-перше, наглядовий орган зазначив, що системи обліку робочого часу, які використовують відбитки пальців, є системами, які обробляють біометричні дані.

Наглядовий орган зазначив, що, ця система здатна пов'язувати характеристики відбитка пальця суб'єкта даних із кодом, який ідентифікує лише одного суб'єкта даних. Це означає, що відбиток пальця служить «унікальним ідентифікатором».

Таким чином, за даними наглядового органу, немає сумнівів, що відбитки пальців підпадають під визначення біометричних даних, наведене в статті 4(14) GDPR.

По-друге, наглядовий орган нагадав, що обробка біометричних даних підпадає під дію статті 9 GDPR. Таким чином, контролер не може посилатися на правову підставу, передбачену статтею 6(1)(c) GDPR , але повинен довести, що обробка підпадає під один із винятків, перелічених у статті 9(2) GDPR.

Оскільки контролер посилався на існування юридичного зобов'язання, наглядовий орган оцінив, чи може відповідна обробка здійснюватися відповідно до статті 9(2)(b) GDPR . У наглядовому органі зазначили, що в чинному національному законодавстві та колективному договорі не зазначено, що контролер повинен використовувати таку систему обліку часу.

Таким чином, наглядовий орган дійшов висновку, що така обробка, не підпадає під жодну правову підставу відповідно до GDPR. Як наслідок, було встановлено порушення статті 5(1)(a) GDPR у поєднанні зі статтею 9 GDPR.

По-третє, наглядовий орган не погодився з аргументацією контролера щодо відсутність оцінки впливу на конфіденційність. На відміну від заяви контролера, наглядовий орган виявив, що обробка дійсно включала дані статті 9 GDPR.

Зокрема, було зазначено, що стаття 35(3)(b) GDPR вимагає проведення оцінки впливу на конфіденційність,

коли йдеться про обробку спеціальних категорій персональних даних.

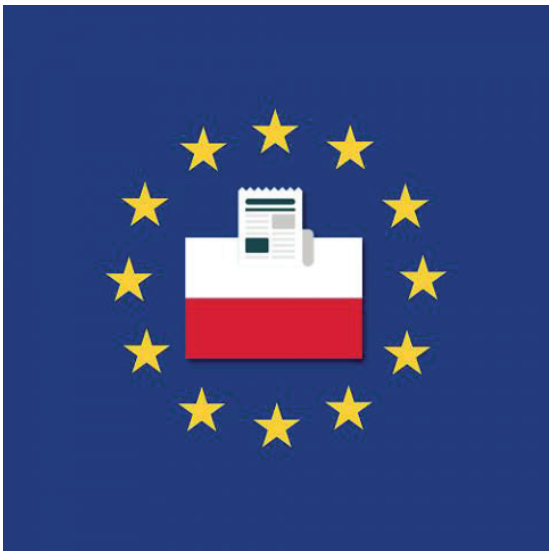
Нарешті, наглядовий орган зазначив, що відповідно до статті 35(4) GDPR 6 травня 2019 року він опублікував перелік операцій обробки, які підлягають проведенню оцінки впливу на конфіденційність. Серед перелічених операцій обробки можна знайти операції обробки, які включають спеціальні категорії персональних даних, включаючи біометричні дані.

Таким чином, наглядовий орган постановив, що в цьому випадку контролеру потрібно було б провести оцінку впливу на конфіденційність, і виявив порушення статті 35(1) GDPR.

На цих підставах наглядовий орган наказав контролеру вжити коригувальних заходів, які полягають у впровадженні системи обліку робочого часу, яка не використовує відбитки пальців.

30. UODO (Польща)[31]

Наглядовий орган:	UODO (Польща)
Юрисдикція:	Польща
Відповідний закон:	Стаття 5(1)(f) GDPR Стаття 5(2) GDPR Стаття 24(1) GDPR Стаття 32(1) GDPR Стаття 32(2) GDPR
Тип справи:	Розслідування
Результат:	Виявлено порушення
Дата рішення:	13.08.2024
Штраф:	1 440 549 злотих



Резюме справи

Група хакерів атакувала одну з польських компаній медичного сектору - American Heart of Poland SA. Хакери встановили шкідливе програмне забезпечення. Постраждали приблизно 21 000 співробітників і пацієнтів компанії і було отримано доступ до наступних наборів персональних даних:

- Прізвище, ім'я, по-батькові, дата народження, адреса електронної пошти, телефон.
- Адреса проживання.

[31] *https://gdprhub.eu/index.php?title=UODO_(Poland)_-_DKN.5112.35.2021*

- Номер PESEL, ідентифікаційний номер.
- Номер банківського рахунку, фінансові дані.
- Дані про здоров'я.
- Дані облікового запису користувача компанії.

Хакери вимагали викуп у розмірі 3 мільйонів доларів США. Щоб змусити компанію заплатити викуп, хакери поділилися зразком отриманих даних на сайті Darknet.

Через втрату доступу та конфіденційності даних компанія, яка діє як контролер даних, повідомила наглядовому органу з питань захисту персональних даних Польщі (UODO) про порушення відповідно до статті 33 GDPR. У відповідь наглядовий орган почав розслідування.

Спочатку контролер не знайшов джерело витоку даних. Однак після поглибленого аналізу зовнішніми фахівцями виявилося, що до зламу призвела відсутність оновлення програмного забезпечення компанії. IT-відділ компанії, відповідальний за оновлення, цього не зробив. Крім того, в якості потенційного джерела зламу вказувалися неналежна якість паролів і фішингова атака.

Контролер даних брав активну участь у врегулюванні результатів витоку даних, серед іншого, сприяючи контакту із суб'єктами даних (через спеціальний колл-центр).

Наглядовий орган визнав, що контролер порушив статтю 5(1)(f) GDPR , статтю 5(2) GDPR , статтю 24(1) GDPR, статтю 32(1) GDPR і статтю 32(2) GDPR.

По-перше, контролер не оцінював ризики обробки даних до порушення безпеки даних. Контролер відніс більшість процесів обробки до низького та середнього рівня ризику, незважаючи на те, що контролер не запровадив політику оцінки ризиків і вжиття відповідних заходів безпеки.

По-друге, контролер регулярно не тестував і не перевіряв діючі організаційні заходи та технічні заходи безпеки, а також не запровадив для цього відповідну внутрішню політику. У результаті наглядовий орган виявив прогалини у заходах безпеки, серед іншого, посилаючись на конфігурацію домену, особливо доступ до домену (доступ адміністратора встановлено як параметр за замовчуванням) і використовуване програмне забезпечення. Крім того, контролер не зміг визначити джерело витоку даних.

Вищезазначена поведінка призвела до того, що контролер не вжив належних технічних та організаційних заходів відповідно до статті 32 GDPR. Наглядовий орган підкреслив, що більшість виявлених недоліків безпеки все ще були наявні після витоку даних під час розслідування.

У результаті контролера оштрафували на 1 440 549 злотих (330 000 євро) і зобов'язали привести операції з обробки даних у відповідність до відповідних положень GDPR, зокрема, шляхом впровадження відповідних технічних та організаційних заходів. Наглядовий орган, приймаючи рішення про розмір штрафу, враховував, зокрема, недбалість контролера, яка сприяла порушенню, та попередні порушення положень GDPR, вчинені контролером.