ISSN 2078-4503. Вісник Львівського університету. Серія юридична. 2024. Випуск 78. С. 190–202
Visnyk of the Lviv University. Series Law. 2024. Issue 78. P. 190–202

УДК 342.5:341.1

АДМІНІСТРАТИВНО-ПРАВОВИЙ ОРГАНІЗАЦІЙНИЙ МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄС

Ростислав Пристай

Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, Україна,79000,
email: rostyslav.council@gmail.com
ORCID ID: 0000-0002-8980-1650

Захист персональних даних станом на сьогодні є однією з основних сфер юридичної діяльності, яка має на меті захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, пов'язаного з обробкою персональних даних. У рамках Європейського Союзу створений та активно функціонує специфічний механізм правового регулювання захисту інформації про особу. Зазначений механізм складається із системи нормативно-правових актів, які запроваджують та регулюють діяльність системи органів виконавчої влади Європейського Союзу та держав-членів, а саме організаційного (інституційного) механізму захисту персональних даних. Інституційний механізм, починаючи з травня 2018-го р. (вступу в дію Загального Регламента про захист даних – GDPR), доводить свою високу ефективність, зважаючи на кількість штрафів, накладених у зв'язку з порушенням контролерами та процесорами законодавства про захист персональних даних та створене сприятливе для захисту права на приватне життя (в частині автоматизованої обробки даних та створення картотек даних) середовище. На противагу цьому, з прийняттям Угоди про Асоціацію між Україною та ЄС, система захисту персональних даних в Україні залишилася практично незмінною, і функціонує на основі законодавства, яке було прийнято до набрання чинності новим законодавством ЄС у цій сфері. Зважаючи на необхідність перегляду національного законодавства в цій сфері, виникає потреба в дослідженні, описі та аналізі наявної системи функціонування вказаного механізму захисту даних в ЄС, а саме інституційного механізму.

Ключові слова: захист персональних даних, право Європейського Союзу, адміністративно-правовий механізм, Європейська комісія, Європейська рада з захисту даних, національні органи з захисту даних.

DOI: http://dx.doi.org/10.30970/vla.2024.78.190

Вступ. Станом на сьогодні, система захисту персональних даних в Україні складається із конституційного, цивільно-правового, адміністративного та кримінально-правового механізмів захисту даних. Нормативною базою для функціонування вказаних механізмів виступають норми Конституції України [1] (наприклад, ст. 32 «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України»), а також норми Закону України «Про захист персональних даних» від 1 червня 2010 р. [2], який був прийнятий на виконання норм Директиви Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Додаткового протоколу до неї щодо органів нагляду та транскордонних потоків даних [3] (ратифікованих Законом України від 6 липня 2010 р. №2438-VI), а також Директиви 95/46/ЕС Європейського Парламенту та Ради від 24 жовтня 1995 р. щодо захисту осіб у зв'язку з обробкою персональних даних та щодо вільної передачі таких даних [4].

Основою функціонуваня всієї системи захисту персональних даних в Україні є норми Закону, прийнятого в 2010-му р., незважаючи на те, що 24 травня 2016 р., в рамках Європейського Союзу було прийнято цілком новий нормативно-правовий акт, а саме Загальний регламент про захист даних [5] (General Data Protection Regulation (GDPR) (EU) 2016/679). Відтак, починаючи з 2016-го р., а в деяких державах-членах ЄС з 1995-го р., механізми захисту персональних даних суттєво відрізняються від наявних в Україні. Так, у рамках ЄС було запроваджено посаду Офіцера з захисту даних, Європейського інспектора з захисту даних (запроваджено в 2001 р.), а також покладено обов'язок на держав-членів щодо створення національних органів з захисту персональних даних (*Data Protection Authorities*). Відтак можемо простежувати суттєву зміну самої системи функціонування органів виконавчої влади в цій сфері, що відноситься в основному до адміністративно-правового механізму захисту персональних даних.

Постановка проблеми. З прийняттям Угоди при Асоціацію між Україною та Європейським Союзом у березні 2014-го р., відповідно до ст. 15 Угоди [6], Україна взяла на себе зобов'язання здійснювати забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських стандартів. Однак після десяти років від часу прийняття відповідного зобов'язання, законодавство про захист персональних даних так і не було вдосконалено. Результатом є відсутність окремого органу з моніторингу дотримання законодавства про захист персональних даних, відсутність координації між суб'єктом даних та розпорядником таких даних, а також застарілі норми, зокрема, понятєвий апарат самого Закону про захист даних.

Зважаючи на необхідність та невідворотність зміни національного законодавства про захист персональних даних в Україні, постає питання про проведення аналізу іноземного досвіду у сфері захисту персональних даних, зокрема, в рамках адміністративно-правового (публічно-владного) механізму. Дослідження вказаного механізму дозволить повно та якісно вивчити організаційну систему захисту персональних даних в ЄС та побудувати відповідні рекомендації щодо доцільності та ефективності запровадження її елементів у законодавство України в межах прийняття нового законодавства про захист персональних даних.

Аналіз останніх досліджень та публікацій. Організаційні механізми захисту персональних даних досліджували такі науковці, як М. М. Бліхар, Т. О. Гуржій, А. Л. Петрицький, Р. В. Ігонін, О. Шевчук О. та ін. Увага вітчизняних авторів зосереджена на механізмах захисту персональних даних у рамках національної правової системи. В цій статті розкрито особливості побудови відповідної системи в межах саме Європейського Союзу.

Постановка завдання. Мета статті полягає в описі особливостей побудови та функціонування адміністративно-правового організаційного механізму захисту персональних даних в ЄС, його ефективності у сфері захисту персональних даних суб'єктів даних (громадян ЄС) та формулюванні висновків щодо доцільності запровадження елементів вказаного механізму в законодавство України.

Основний виклад матеріалу. В цій статті досліджується саме організаційна складова адміністративно-правового механізму захисту персональних даних. Вказану складову автор розглядає як *підсистему адміністративного механізму правового регулювання захисту персональних даних, що містить відповідні регулятивні та насамперед інституційні правові засоби (механізми реалізації права), за допомогою яких здійснюється захист персональних даних особи в Європейському Союзі.*

Під організаційними механізмами слід мати на увазі складові інституційної системи адміністративно-правового регулювання. До органів публічного адміністрування (адміністративних органів) заведено відносити суб'єктів, які мають організаційну структуру публічного адміністрування, під яким розуміється органічно єдина та чинна система органів державного управління, передусім органів виконавчої влади та владних структур місцевого самоврядування, їх посадових і службових осіб, а також установ, організацій, окремих недержавних структур, які відповідно до законодавства здійснюють публічні управлінські функції з метою задоволення публічного інтересу. Відповідно до ст. 2 Закону України «Про адміністративну процедуру», до них належать, наприклад, *органи виконавчої влади, органи місцевого самоврядування, їх посадові особи та інші суб'єкти, які відповідно до закону уповноважені здійснювати функції публічної адміністрації (надання адміністративних послуг, здійснення інспекційної (контрольної, наглядової) діяльності, вирішення інших справ за заявою особи або за власною ініціативою адміністративного органу).* За вказаним критерієм автором статті досліджено відповідні механізми захисту персональних даних в Європейському Союзі.

Складові наднаціонального адміністративно-правового організаційного механізму захисту персональних даних в ЄС. Враховуючи природу Європейського Союзу як міжнародної організації особливого роду *sui generis* з відповідною ієрархією правових актів ЄС, системою наднаціональних органів ЄС та національних органів держав-членів, доцільним є дослідження адміністративно-правових механізмів захисту персональних даних на двох рівнях – загальносоюзному та національному.

Нормативна основа функціонування. Основними нормативно-правовими актами, які опосередковують діяльність адміністративних органів захисту персональних даних на рівні Європейського Союзу, є Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних (Загальний регламент про захист даних (GDPR, надалі – Регламент)); Регламент (ЄС) 2018/1725 Європейського Парламенту та Ради від 23 жовтня 2018 р. про захист фізичних осіб щодо обробки персональних даних інституціями, органами, офісами та агентствами Союзу та про вільне переміщення таких даних [7] та Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування правопорушень або виконання кримінальних покарань, а також щодо вільного переміщення таких даних [8]. Зазначеними актами створено Європейську раду з захисту даних (Регламент), Європейського інспектора з захисту даних та посаду Уповноваженого із захисту даних Європейської комісії. Втім, слід зазначити і про важливість практичної діяльності Європейської комісії загалом, як вищого органу виконавчої влади в ЄС, яка виступає основним суб'єктом законодавчої ініціативи в цій сфері. Вказані органи є основними елементами адміністративно-правового організаційного механізму захисту персональних даних на рівні ЄС. Розкриємо мету їх діяльності, повноваження, структурні підрозділи та приклади з практичної діяльності у сфері захисту персональних даних.

Європейська рада із захисту даних (надалі – Рада). Із прийняттям Загального регламенту про захист даних, ст. 68 Регламенту, було засновано Європейську раду захисту даних як самостійний орган Союзу зі статусом юридичної особи. Рада має

сприяти послідовному застосуванню Регламенту (ЄС) 2016/679 і Директиви (ЄС) 2016/680 в усьому Союзі, зокрема шляхом консультування Комісії.

Рада складається з голови одного наглядового органу кожної держави-члена Союзу та Європейського інспектора із захисту даних, діяльність якого ми розглянемо окремо. Компетенція Ради є широкою і складається з: контролю та забезпеченням правильного застосування Регламенту; консультування Комісії з будь-яких питань, пов'язаних із захистом персональних даних; видачі вказівок та рекомендацій щодо видалення персональних даних із загальнодоступних комунікаційних служб; розгляду за своєю ініціативою або за запитом питань щодо застосування Регламенту та інших контрольних функцій. Рада складає щорічний звіт щодо захисту фізичних осіб щодо обробки в Союзі та, у відповідних випадках, у третіх країнах і міжнародних організаціях. Звіт оприлюднюється та передається до Європейського Парламенту, Ради та Комісії.

Приклади діяльності. Європейська рада із захисту даних (EDPB) 15 лютого 2023 р. вперше розпочала спільну скоординовану дію. Перший скоординований примусовий захід спрямований на використання державним сектором хмарних послуг. Відповідно до цього заходу 22 наглядові органи, включно з Європейським інспектором із захисту даних, звертатимуться до понад 80 державних органів у всій Європейській економічній зоні (ЄЕЗ), включаючи установи ЄС. Дія охоплюватиме широкий спектр секторів (наприклад, охорона здоров'я, фінанси, податки, освіта, центральні покупці або постачальники IT-послуг), з метою вивчення проблем, з якими вони стикаються у зв'язку з дотриманням Загального регламенту захисту даних під час використання хмарних послуг. За результатами наглядові органи приймуть рішення щодо можливого додаткового державного нагляду та примусових дій. Отримані знання також можуть бути використані для цільових подальших заходів на рівні ЄС.

Рада 13 лютого 2024 р. також прийняла Висновок 04/2024 щодо поняття основного представництва контролера в Союзі згідно зі ст. 4(16)(a) Загального регламенту ЄС щодо захисту даних [8] («Висновок»). Висновок був надісланий Управлінням із захисту даних Франції («CNIL») і спрямований на роз'яснення поняття «основного представництва» контролера даних у ЄС у значенні ст. 4(16)(a) GDPR. Ст. 4(16)(a) визначає поняття «головна установа» таким чином: «місце її центрального управління в Союзі, якщо рішення щодо цілей і засобів обробки персональних даних не приймаються в іншій установі контролер у Союзі, а остання установа має повноваження виконувати такі рішення, і в цьому випадку установа, яка прийняла такі рішення, вважається головною установою». Основна концепція створення є наріжним каменем принципу «єдиного вікна» GDPR, оскільки вона має ключове значення для визначення того, який із органів ЄС із захисту даних, якщо такі є, є провідним наглядовим органом у транскордонних справах щодо захисту даних.

Європейський інспектор із захисту даних. Ч. 3 ст. 1 Регламенту (ЄС) 2018/1725 Європейського Парламенту та Ради від 23 жовтня 2018 р. про захист фізичних осіб щодо обробки персональних даних інституціями, органами, офісами та агентствами Союзу та про вільне переміщення таких даних визначено, що Європейський інспектор із захисту даних контролює застосування положень цього Регламенту до всіх операцій з обробки, які здійснюються установою чи органом Союзу. Ч. 3 ст. 52 вказаного Регламенту деталізує це положення, а саме зазначає, що Європейський інспектор із захисту даних несе відповідальність за моніторинг та забезпечення застосування положень цього Регламенту *та будь-якого іншого*

акта Союзу, що стосується захисту основних прав і свобод фізичних осіб щодо обробки персональних даних Союзом установи чи органу, а також для консультування установ і органів Союзу та суб'єктів даних з усіх питань, що стосуються обробки персональних даних.

Завдання і повноваження Європейського інспектора із захисту даних визначені ст.ст. 57 і 58 Регламенту. Серед завдань, зокрема проведення розслідувань щодо застосування цього Регламенту, зокрема на основі інформації, отриманої від іншого контролюючого органу чи іншого органу державної влади та ведення внутрішніх записів про порушення цього Регламенту та заходи, вжиті відповідно до ст. 58(2). До компетенції ж відносяться а) наказ контролеру та процесору надати будь-яку інформацію, необхідну для виконання його або її завдань; (б) проводити розслідування у формі аудиту захисту даних; (c) повідомляти контролера або процесора про ймовірне порушення цього Регламенту; (d) отримувати від контролера та обробника доступ до всіх персональних даних та до всієї інформації, необхідної для виконання його або її завдань; (д) отримати доступ до будь-яких приміщень контролера та процесора, включаючи будь-яке обладнання та засоби обробки даних, відповідно до законодавства Союзу. Для забезпечення виконання повноважень, Європейський інспектор із захисту даних має повноваження передавати справу до Суду відповідно до умов, передбачених Договорами, і втручатися в позови, подані до Суду.

Європейські органи та установи звертаються до Європейського інспектора із захисту даних за порадою через своїх спеціалістів із захисту даних (DPO). Деякі з цих консультацій є обов'язковими, інші – добровільними. Поради надаються у висновках, коментарях, рішеннях, листах або документах і вказівках. Прикладом є Висновок Європейського інспектора із захисту даних щодо попередніх консультацій на запит агентства ЄС зі співпраці правоохоронних оганів (Європол) про рішення для розпізнавання обличчя [9]. Так, Європейський інспектор із захисту даних вважає за необхідне, щоб Європол запровадив «пілотний» підхід до обробки зображень обличчя за допомогою нового інструменту розпізнавання обличчя, щоб гарантувати, що обробка зображень обличчя, як спеціальної категорії персональних даних згідно зі ст. 30(2) ER, залишалася суворо пропорційною. Цей пілотний проєкт має дозволити приймати рішення на основі доказів щодо того, який поріг збігу та/або числове обмеження ще більше зменшать ризики для суб'єктів даних, одночасно дозволяючи Агентству досягти запланованої мети рішення для розпізнавання облич.

Уповноважений із захисту даних в Європейській комісії. Зазначена посада введена Регламентом (ЄС) № 45/2001 Європейського Парламенту та Ради від 18 грудня 2000 р. про захист осіб щодо обробки персональних даних установами та органами Співтовариства та про вільний рух таких даних – хоч Регламент втратив чинність, у цій частині він є застосовним і надалі [10]. Кожна установа та орган Співтовариства призначає принаймні одну особу уповноваженою особою із захисту даних. Ця посада є аналогічною посаді Офіцера з захисту персональних даних, які здійснюють контроль за додержанням Регламента на підприємствах, установах, організаціях держав-членів (на національному рівні).

Уповноважений із захисту даних (DPO) незалежно забезпечує правильне застосовування Комісією закону про захист персональних даних фізичних осіб, і веде публічний реєстр усіх операцій, які проводить Комісія з персональними даними. Уповноважений Комісії із захисту даних публікує реєстр усіх операцій з обробки персональних даних Комісією, які були задокументовані та повідомлені йому.

Прикладом такого запису є Запис про захист даних DPR-EC-00932.1 «Система обміну інформацією Європейської міграційної мережі» [11], який містить коментарі та додаткову інформацію до інформації, наданої суб'єктам даних про їхні права: зокрема інформацію про суб'єктів даних, категорії інформації, яка підлягає обробці, реципієнтів, положення про транскордонну передачу даних та заходи безпеки. Так, Європейська міграційна мережа (EMN) була створена Рішенням Ради (2008/381/ЄС) і має як правову основу ст. 74 ДФЄС (колишня ст. 66 ДЄС). Мета EMN полягає в тому, щоб задовольнити інформаційні потреби інституцій ЄС і держав-членів з питань міграції та притулку шляхом надання актуальної, об'єктивної, надійної та порівняльної інформації про міграцію та притулок. Норвегія та Швейцарія також беруть участь у роботі EMN. EMN, зокрема, збирає та обмінюється даними з широкого кола джерел, проводить аналіз таких даних, а також координує інформацію та співпрацює з іншими відповідними європейськими та міжнародними органами. Згідно з п. (e) ст. 2(1) Рішення Ради, EMN створює та підтримує систему обміну інформацією в інтернеті, яка забезпечує доступ до відповідних документів і публікацій у сфері міграції та притулку.

Як вказано в записі, передача даних користувачів необхідна з міркувань суспільного інтересу, щоб забезпечити співпрацю між відповідними зацікавленими сторонами у сфері міграції. Законодавство ЄС визнає суспільний інтерес Союзу в ефективному управлінні міграцією та зміцненні співпраці органів влади та відповідних зацікавлених сторін. Усі користувачі, увійшовши в IES вперше, погодилися на обробку своїх персональних даних відповідно до умов використання, а отже, прямо дали згоду на передачу персональних даних.

Отож у рамках ЄС кожна обробка персональних даних інституціями та органами реєструється онлайн і знаходиться у відкритому доступі з обґрунтуванням її найважливіших аспектів, які можуть становити інтерес для суб'єкта даних.

До інших повноважень Уповноваженого із захисту даних належать: забезпечення незалежно внутрішнього застосування Регламенту (ЄС) 2018/1725 у Комісії; інформування та консультування департаментів Комісії та їхнього персоналу щодо їхніх зобов'язань щодо захисту даних; гарантування, що права та свободи суб'єктів даних не зазнають негативного впливу операцій з обробки департаментами Комісії та співпраця з Європейським інспектором із захисту даних.

Діяльність Європейської комісії у сфері захисту персональних даних в ЄС. Незважаючи на те, що Комісія напряму не виступає органом, який безпосередньо здійснює захист персональних даних, вона все ж є частиною органів виконавчої влади ЄС (головним органом виконавчої влади) і єдиним органом, відповідальним за розробку пропозицій щодо нового європейського законодавства та виконання рішень Європейського парламенту та Ради ЄС (зокрема, в частині моніторингу розвитку національного законодавства в цій сфері). В цій статті зосередимо увагу саме на контрольно-наглядовій функції Комісії, яка стосується виконання положень GDPR державами-членами ЄС.

Указана функція стосується передачі персональних даних третім країнам або міжнародним організаціям. Відтак міжнародна передача може мати місце, якщо Комісія вирішила, що третя країна, територія або один чи більше визначених секторів у цій третій країні, або міжнародна організація, про яку йдеться, забезпечує адекватний рівень захисту. Варто зазначити, що у випадку прийняття такого рішення Комісією, відповідна передача не вимагає спеціального дозволу суб'єкта даних (лише інформування). При прийнятті вказаного рішення Комісія бере до уваги наступні фактори: а) верховенство права, повагу до прав людини та основних свобод у державі; б) наявність

та ефективне функціонування одного чи кількох незалежних національних контрольно-наглядових органів з захисту персональних даних; в) міжнародні зобов'язання, які взяла на себе міжнародна організація або третя країна.

Комісія, після оцінки відповідності рівня захисту, може вирішити за допомогою імплементаційного акта, що третя країна, територія або один чи більше визначених секторів у третій країні, або міжнародна організація забезпечує належний рівень захисту. Імплементаційний акт передбачає механізм періодичного перегляду, принаймні кожні чотири роки, який бере до уваги всі відповідні події в третій країні або міжнародній організації. В імплементаційному акті вказується його територіальне та галузеве застосування та, якщо це застосовно, ідентифікується наглядовий орган або органи.

Комісія повинна на постійній основі стежити за розвитком подій у третіх країнах та міжнародних організаціях. Комісія публікує в Офіційному журналі Європейського Союзу та на своєму вебсайті [12] перелік третіх країн, територій і визначених секторів у третій країні та міжнародних організаціях, для яких вона вирішила, що адекватний рівень захисту є або більше не є забезпеченим.

Складові національного адміністративно-правового організаційного механізму захисту персональних даних в ЄС. Аналогічно з наднаціональним, національний адміністративно-правовий механізм захисту персональних даних також регулюється положеннями Регламенту про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних; Регламентом про захист фізичних осіб щодо обробки персональних даних інституціями, органами, офісами та агентствами Союзу та про вільне переміщення таких даних та Директивою про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування правопорушень або виконання кримінальних покарань, а також щодо вільного переміщення таких даних.

Так, ст. 37 Регламенту зобов'язує контролера або розпорядника призначити офіцера з захисту даних у визначених ч.1 цієї статті випадках. Своєю чергою, ст. 51 покладає обов'язок на держав-членів щодо створення незалежного контролюючого органу, відповідального за моніторинг дотримання положень Регламенту. Відповідні положення вказаних нормативно-правових актів продубльовані в національному законодавстві – сюди належать, наприклад, Закон про захист персональних даних у Німеччині (BDSG – Bundesdatenschutzgesetz, секція 8 – Федеральний уповноважений із захисту даних і свободи інформації), Закон про захист персональних даних у Франції (Loi Informatique et Libertés – Національна комісія з питань інформатики та свободи – CNIL), Закон про захист персональних даних в Італії (Закон No. 675 від 31 грудня 1996 р. та Codice in materia di protezione dei dati personali, які регулюють запровадження органу Гаранта захисту персональних даних), Закон про захист персональних даних у Польщі (Ustawa o Ochronie Danych Osobowych, який запроваджує створення Управління та посаду Президента Управління захисту персональних даних) тощо).

Відтак основним і, практично, єдиним елементом, який характеризує адміністративно-правовий механізм захисту персональних даних на рівні держав-членів ЄС, є національні органи захисту персональних даних. Указаний механізм опосередкований вимогами ст. 51-53 GDPR щодо незалежності вказаних органів від системи органів виконавчої, законодавчої та судової влади. Варто зауважити, що рішення національних органів захисту персональних даних можуть бути об'єктом перегляду національними судами (зокрема, адміністративними), а позови проти

контролера або процесора подаються в судах держави-члена, де контролер або процесор має установу. Втім об'єктом нашого дослідження є саме органи виконавчої влади, а тому увага буде зосереджена саме на них.

Національні органи з захисту персональних даних (supervisory authorities або ж National Data Protection Authorities). Як було зазначено, ст. 51 Регламенту зобов'язує держав-членів передбачити один або більше незалежних державних органів, відповідальних за моніторинг застосування цього Регламенту з метою захисту основних прав і свобод фізичних осіб у зв'язку з обробкою та сприяння вільному потоку персональних даних у межах Союзу. Повноваження вказаних органів визначені ст.ст. 56–59 Регламенту. До їх завдань та повноважень, які характерні саме для функції безпосереднього захисту персональних даних в адміністративному порядку, належать, зокрема:

1) моніторинг та забезпечення виконання Регламенту;

2) розгляд скарг, поданих суб'єктом даних або органом, організацією чи асоціацією відповідно до ст. 80, і розслідування, відповідною мірою, предмета скарги та інформування скаржника про хід і результати розслідування протягом розумного періоду, зокрема, якщо необхідне подальше розслідування або узгодження з іншим наглядовим органом;

3) проведення розслідування щодо застосування Регламенту, зокрема на основі інформації, отриманої від іншого контролюючого органу чи іншого органу державної влади;

4) стеження за відповідними розробками, наскільки вони впливають на захист персональних даних, зокрема розвиток інформаційних і комунікаційних технологій і комерційної практики;

5) ведення внутрішніх записів про порушення Регламенту та заходи, вжиті відповідно до ст. 58(2).

Решта завдань (сукупно ст. 57 Регламенту передбачено 22 завдання, але список є невиключним) також спрямовані на захист прав та свобод суб'єктів даних, однак опосередковано – через створення та затвердження механізмів сертифікації, сприяння кооперації між національними органами, надання порад щодо застосування статей Регламенту, сприяння усвідомленню контролерів та обробників їхніх зобов'язань тощо.

Зауважимо, що найбільш впливовим інструментом примусу, який може бути застосований згідно з Регламентом національними органами, є накладення штрафів, передбачених ст. 83 Регламенту і можуть досягати 20-ти мільйонів євро та 4% від світового річного обороту компаній.

Так, максимальну суму штрафу, наприклад, було застосовано Італійським органом з захисту персональних даних. Орган з захисту персональних даних Італії розпочав провадження за власним бажанням після повідомлень у пресі про кілька проблем, пов'язаних із продуктами розпізнавання обличчя, які пропонує компанія *Clearview AI Inc*. Крім того, протягом 2021 р. *Garante* отримала чотири скарги та два попередження від двох організацій, які працюють у сфері захисту конфіденційності та основних прав осіб проти *Clearview.*

Розслідування та оцінка виявили кілька порушень з боку *Clearview AI Inc*. Персональні дані, які зберігаються компанією, включно з біометричною та геолокаційною інформацією, оброблялися незаконно без відповідної правової підстави, оскільки законний інтерес американської компанії не кваліфікується як такий на території Італії [13]. Крім того, компанія порушила кілька основних принципів GDPR, таких як прозорість, обмеження цілей і обмеження зберігання; не було

надано інформацію, викладену у ст. 13–14, не надано інформацію про дії, вжиті за запитом згідно зі ст. 15, протягом належного терміну та не визначено представника в ЄС. Італійський орган наклав штраф у розмірі 20 мільйонів євро. Крім того, він визначив наступне:

– наклав заборону на будь-який подальший збір, за допомогою методів веб-збирання, зображень і відповідних метаданих, що стосуються осіб на території Італії, а також на подальшу обробку стандартних і біометричних даних, які обробляються Компанією через її систему розпізнавання облич і концерн особи на території Італії;

– наказав стерти дані, включаючи біометричні дані, оброблені його системою розпізнавання обличчя стосовно осіб на території Італії, за умови зобов'язання своєчасно відповідати на такі запити для реалізації прав згідно зі ст. 15–22 Регламенту, як могли бути отримані від суб'єктів даних відповідно до ст. 12(3) Регламенту;

– наказав Компанії призначити представника на території Європейського Союзу.

Висновки. Дослідивши діяльність адміністративного інституційного механізму захисту персональних даних в Європейському Союзі, можемо побудувати наступні висновки:

1. Основними складовими адміністративно-правового організаційного механізму захисту персональних даних у рамках Європейського Союзу є: Європейська рада з захисту даних, Європейський інспектор з захисту даних, Європейська комісія, Уповноважений із захисту даних в Європейській комісії та національні органи з захисту персональних даних.

2. Можемо виокремити два напрями в контексті діяльності вказаних органів – захист персональних даних суб'єкта даних тоді, коли обробка відбувається інституціями, органами, офісами та агентствами Союзу (в рамках Регламенту (ЄС) 2018/1725 Європейського Парламенту та Ради від 23 жовтня 2018 р. про захист фізичних осіб щодо обробки персональних даних інституціями, органами, офісами та агентствами Союзу та про вільне переміщення таких даних) та в межах, передбачених ст.ст. 2, 3 Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних – коли здійснюється обробка персональних даних повністю або частково автоматизованими засобами, а також обробка неавтоматизованими засобами персональних даних, які є частиною картотеки або призначені для створення картотеки за винятком випадків, передбачених ч. 2 ст. 2 Регламенту;

3. Основою функціонування всієї системи захисту персональних даних, яка регулюється GDPR, у рамках адміністративно-правового механізму захисту даних, є національні органи захисту персональних даних та Європейська Рада з захисту даних. Указані органи здійснюють розгляд скарг і розслідування, відповідною мірою, предмета скарги та інформування скаржника про хід і результати розслідування, саме тоді як Рада видає рекомендації та вказівки щодо застосування Регламенту і складає щорічний звіт щодо захисту фізичних осіб щодо обробки в Союзі та, у відповідних випадках, у третіх країнах і міжнародних організаціях.

4. Національні суди не є частиною органів виконавчої влади і не належать до адміністративно-правового механізму захисту персональних даних. Однак, як це передбачено Регламентом, вони уповноважені здійснювати перегляд рішень (зокрема накладення штрафів чи інших засобів примусу) національних органів з захисту персональних даних в особливій, встановленій законом, процесуальній

формі і під час перевірки правильності рішення органів, предметом їх розгляду є, зокрема, обставини справи, які були досліджені DPA.

5. Описані приклади ефективності адміністративно-правового механізму захисту персональних даних в ЄС вказують на необхідність створення окремого органу з захисту персональних даних, зокрема, і в Україні, який зможе ефективно впливати на захист персональних даних в Україні і створить сприятливе для забезпечення безпеки персональних даних середовище. З цією метою необхідно здійснити перегляд ефективності функціонування Уповноваженого Верховної Ради України з прав людини в цій сфері та розглянути можливість покладення вказаних функцій на окремий орган. Також варто переглянути положення Закону України «Про захист персональних даних» на предмет його відповідності вимогам Загального регламенту даних відповідно до нормативних вимог Угоди про асоціацію з ЄС, який був прийнятий та набув чинності через вісім років після прийняття закону, який станом на сьогодні діє в Україні.

Список використаних джерел

1. Конституція України, прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. *Відомості Верховної Ради України*. URL: http://zakon2.rada.gov.ua/laws/show/254к/96-вр.
2. Про захист персональних даних : Закон України від 01.06.2010 р. URL: https://zakon.-rada.gov.ua/laws/card/2297-17.
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, European Treaty Series - No. 108, available at. URL: https://rm.coe.int/1680078b37.
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?-uri=CELEX%3A31995L0046.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
6. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 16.09.2014 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text.
7. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, available at. URL: https://eur-lex.europa.eu/eli/reg/2018/1725/oj.
8. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, available at. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A-32016L0680.
9. The opinion of the European Data Protection Supervisor on the preliminary consultations at the request of the EU Agency for Law Enforcement Cooperation (Europol) on facial recognition solutions, available at. URL: https://www.edps.europa.eu/system/files/2024-01/2023-1247_d0187_opinion_en.pdf.

10. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, available at. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045.
11. Запис про захист даних DPR-EC-00932.1 «Система обміну інформацією Європейської міграційної мережі». URL: https://ec.europa.eu/dpo-register/detail/DPR-EC-00932.1.
12. Офіційний веб-сайт Європейського Союзу зі списком держав, які забезпечують адекватний рівень захисту персональних даних. URL: https://commission.europa.-eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Location data is personal data - noyb wins appeal against Spanish DPA, 25 January 2023, noyb webiste. Available at. URL: https://noyb.eu/en/location-data-personal-data-noyb-wins-appeal-against-spanish-dpa.

References

1. Konstytutsiia Ukrainy, pryiniata na piatii sesii Verkhovnoi Rady Ukrainy 28 chervnia 1996 r. Vidomosti Verkhovnoi Rady Ukrainy. Retrieved from : http://zakon2.rada.gov.ua/laws/show/-254k/96-vr (accessed: 15.04.2024) (in Ukrainian).
2. *Zakon Ukrainy pro zakhyst personalnykh danykh» vid 01.06.2010 r.* Retrieved from : https://zakon.rada.gov.ua/laws/card/2297-17 (accessed: 16.04.2024) (in Ukrainian).
3. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, European Treaty Series - No. 108.* Retrieved from : https://rm.coe.int/1680078b37 (accessed: 19.04.2024) (in English).
4. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Retrieved from : https://eur-lex.europa.eu/legal-content/EN/TXT/-?uri=-CELEX%3A31995L0046 (accessed: 15.04.2024) (in English).
5. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Retrieved from : https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed: 17.04.2024) (in English).
6. *Uhoda pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony vid 16.09.2014 r.* Retrieved from: https://zakon.rada.gov.ua/laws/show/984_011#Text. Ofitsiinyi portal Verkhovnoi Rady Ukrainy. (accessed: 17.04.2024) (in Ukrainian).
7. *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.* Retrieved from : https://eur-lex.europa.eu/eli/reg/2018/1725/oj (accessed: 15.04.2024) (in English).
8. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680. (accessed: 16.04.2024) (in English).
9. *The opinion of the European Data Protection Supervisor on the preliminary consultations at the request of the EU Agency for Law Enforcement Cooperation (Europol) on facial recognition solutions.* Retrieved from : https://www.edps.europa.eu/system/files/2024-01/2023-1247_d0187_opinion_en.pdf (accessed: 20.04.2024) (in English).

10. *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.* Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045 (accessed: 17.04.2024) (in English).
11. *Zapys pro zakhyst danykh DPR-EC-00932.1 "Systema obminu informatsiieiu Yevropeiskoi mihratsiinoi merezhi".* Retrieved from : https://ec.europa.eu/dpo-register/detail/DPR-EC-00932.1 (accessed: 16.04.2024) (in Ukrainian).
12. *Ofitsiinyi veb-sait Yevropeiskoho Soiuzu zi spyskom derzhav, yaki zabezpechuiut adekvatnyi riven zakhystu personlnykh danykh*. Retrieved from : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed: 15.04.2024) (in English).
13. *Location data is personal data - noyb wins appeal against Spanish DPA. The Spanish Courts annulled a past decision by the Spanish DPA (AEPD), 25 January 2023, noyb webiste.* Retrieved from : https://noyb.eu/en/location-data-personal-data-noyb-wins-appeal-against-spanish-dpa. (accessed: 22.04.2024) (in English).

ADMINISTRATIVE LEGAL ORGANIZATIONAL MECHANISM OF PERSONAL DATA PROTECTION IN THE EU

Rostyslav Prystai

Ivan Franko National University of Lviv,
1, Universytetska Str., Lviv, Ukraine, 79000,
e-mail: rostyslav.council@gmail.com
ORCID ID: 0000-0002-8980-1650

Today, personal data protection is one of the key areas of legal activity aimed to protect fundamental human rights and freedoms, including the right to privacy related to the processing of personal data. Within the European Union, a specific mechanism of legal regulation of personal information protection has been created and is actively functioning. Such mechanism consists of the system of legal acts that introduce and regulate the activities of the system of executive authorities of the European Union and its Member States, namely the organizational (institutional) mechanism for the protection of personal data. The institutional mechanism, since May 2018 (from the date when the General Data Protection Regulation – GDPR, entered into force), has proved to be highly effective, given the number of fines imposed in connection to violations of personal data protection legislation by controllers and processors and the environment created for the protection of the right to privacy (in terms of automated data processing and the creation of filing systems). In contrast, with the adoption of the EU-Ukraine Association Agreement, the personal data protection system in Ukraine has remained virtually unchanged and operates on the basis of legislation adopted before the entry into force of the new EU legislation in this area. However, in accordance with Article 15 of the Agreement, Ukraine undertook to ensure an adequate level of personal data protection in accordance with the highest European standards. Ten years after the adoption of the relevant commitment, the personal data protection legislation has not been improved. The result is the absence of a separate body to monitor compliance with personal data protection legislation, lack of coordination between the data subject and the data controller, and outdated regulations, including the conceptual framework of the Data Protection Law itself. Given the necessity and inevitability of changing the national legislation on personal data protection in Ukraine, the question arises of analyzing foreign experience in the field of personal data protection, in particular, within the framework of the administrative legal (public authority)

mechanism. The study of this mechanism will allow to fully and qualitatively examine the organizational system of personal data protection in the EU and to build appropriate recommendations on the feasibility and effectiveness of introducing its elements into Ukrainian legislation as part of the adoption of new legislation on personal data protection.

Keywords: personal data protection, European Union law, administrative legal mechanism, European Commission, European Data Protection Board, national data protection authorities.

Стаття: надійшла до редакції 28.04.2024
прийнята до друку 30.04.2024