ISSN 1995-6134

УДК 349.22:331.108
М.В. РІЗАК, Державний вищий навчальний заклад «Ужгородський національний університет»

ПРАВОВИЙ СТАТУС УПОВНОВАЖЕНОГО ОРГАНУ З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ: ДОСВІД ЗАРУБІЖНИХ КРАЇН

Ключові слова: *правовий статус, уповноважений орган, питання захисту, персональні данні, досвід, зарубіжні країни*

Одним із провідних напрямів діяльності держави у сфері обігу персональних даних громадян є здійснення контролю над відповідністю процесів їх збору, використання та розпорядження, що здійснюються як на рівні державних (муніципальних), так і приватних структур, вимогам закону. Необхідність наявності такого напрямку обумовлена рядом причин, серед яких слід назвати, перш за все, новизну самого правового інституту персональних даних, не характерного раніше для українського суспільства та держави.

Згідно ст.22 Закону «Про захист персональних даних» контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснює уповноважений державний орган з питань захисту персональних даних [1].

Необхідність створення такого органу була обумовлена змістом міжнародних договорів України, в тому числі Конвенції та Додаткового протоколу до неї про спостережні органи та транскордонну передачу інформації від 08.11.2001 р. Поява такої інституційної одиниці в системі органів влади, безумовно, є більш ніж своєчасним і необхідним заходом, особливо в рамках адміністративно-правової реформи. Його успішне функціонування є запорукою захищеності прав і свобод людини і громадянина при обробці його персональних даних, сприяє підвищенню ступеня свободи громадян, зміцненню правової захищеності і безпеки особи [2, с.72]. Таким чином, метою статті є дослідити окремі особливості правового статусу контролюючого органу за відповідністю процесів збору, використання та розпорядження персональними даними особи, беручи за основу досвід ряду зарубіжних країн.

Основні засади державної інформаційної політики та управління інформаційною сферою розкриті в працях І. Арістової та К. Бєлякова. У контексті концепції захисту прав і свобод людини в останні роки з'явилися праці вітчизняних науковців, в яких досліджуються окремі аспекти проблем реалізації прав людини у сфері інформаційних відносин (В. Гавловський, Р. Калюжний, Б. Кормич, В. Цимбалюк, М. Швець, Г. Чанишева); захисту персональних даних фізичної особи (А. Баранов, В. Брижко, Ю. Базанов, В. Галаган, А. Марущак, О. Жуковська, А. Пазюк, Р. Чанишев, А. Чернобай та ін.).

Отже, розглянемо європейський досвід з цього питання. Так, Регламент Європейського парламенту та Ради № 45/2001 від 18.12.2000 р. про захист прав приватних осіб щодо обробки персональних даних органами та установами ЄС та про вільний рух таких даних (далі – Регламент [3]) у ст.41 заснував новий незалежний інститут Європейського Уповноваженого із захисту даних (далі – Уповноважений ЄС), основним завданням якого є забезпечення поваги прав на недоторканність приватного життя і захисту персональних даних усіма союзними органами та інститутами. Уповноважений відповідальний за забезпечення застосування норм Постанови 45/2001, а також будь-якого іншого союзного акта в сфері персональних даних усіма союзними структурами, а також за консультування останніх з усіх питань обробки персональних даних.

Призначення на цю посаду здійснюється за результатами публічного конкурсу кандидатів. Рішенням Європейського парламенту і Ради від 22.12.2003 р. на 5-річний термін був призначений перший Уповноважений – Пітер Йохан Хустінкс, який займав до цього посаду Президента Голландського агентства із захисту персональних даних. Разом із Уповноваженим на аналогічний термін за тією ж

ISSN 1995-6134

процедурою призначається і його заступник. Таким чином, відлік мандата нової повноважної посадової особи ЄС розпочався з 2004 р. [2, с.73–74].

Один із головних принципів діяльності Уповноваженого – його незалежність – забезпечується за допомогою цілого ряду заходів, передбачених Регламентом 45/2001, серед них вважаємо за потрібне виділити наступні:

1) відповідно до статті 42 (2) кандидат на високу посаду може бути обраний з числа осіб, чия незалежність не викликає сумнівів і хто володіє досвідом і навичками, необхідними для роботи на зазначеній посаді, наприклад в силу їх попередньої участі в роботі національних органів із захисту персональних даних країн-учасниць ЄС;

2) Уповноважений може бути звільнений або позбавлений привілеїв тільки за рішенням Суду Європейських співтовариств на вимогу Європейського парламенту, Ради ЄС або Європейської Комісії, в разі невідповідності вимогам, необхідним для виконання їх обов'язків, або у випадку вчинення посадового злочину;

3) Уповноважений користується всіма привілеями та імунітетами, передбаченими для суддів Суду Європейських співтовариств згідно Протоколу привілеїв та імунітетів ЄС;

4) Уповноважений та його заступник при виконанні своїх обов'язків діють абсолютно незалежно, і не звертаються за вказівками, так само як і не отримують будь-яких вказівок від будь-кого.

В період дії їх мандату вони не можуть займатися діяльністю, несумісною з їх посадовими обов'язками незалежно від того, чи є вона прибутковою чи ні. Крім того, після завершення свого мандата вони повинні з особливою розсудливістю вибирати подальший вид своєї роботи;

5) на Уповноваженого та його штат як в період їх роботи, так і після його завершення поширюється правило про збереження конфіденційності всієї інформації, що стала їм доступною у зв'язку з виконанням своїх посадових обов'язків [3].

Передбачається, що Уповноважений відіграватиме значну роль в політиці щодо захисту персональних даних за допомогою надання своїх консультаційних роз'яснень як за власною ініціативою, так і у відповідь на звернення зацікавлених органів. Зокрема, мова може йти про підготовку рішень або власних норм, пов'язаних з обробкою персональних даних, про що установи повинні інформувати Уповноваженого. Консультаційна функція на вищому рівні проявляється в співпраці з Європейською Комісією з питань прийняття нормативних актів стосовно захисту прав приватних осіб при обробці персональних даних [3, с.75].

Відповідно до ст.46 (1) Постанови 45/2001, Уповноважений заслуховує та розслідує скарги, а також інформує осіб, що звернулися зі скаргою (приватних осіб, про яких або від яких збираються або щодо яких обробляються дані) про своє рішення протягом розумного строку. Означене повноваження кореспондує право кожного суб'єкта даних звертатися до Уповноваженого зі скаргою про порушення права на захист персональних даних, передбачене ст.286 Договору про створення Європейських Співтовариств, будь-якою установою ЄС. У випадку, якщо Уповноважений не надасть відповіді протягом шести місяців з моменту подачі скарги, скарга вважається відхиленою [3].

Регламент 45/2001 передбачає два особливих види скарг Уповноваженому:

1) відповідно до ст.20 Постанови 45/2001 права суб'єктів даних можуть бути обмежені в силу попередження або розслідування злочинів, або в силу особливих економічних інтересів країн-учасниць ЄС, або іншого публічного інтересу. У цьому випадку особа, чиї права обмежені, повинна бути поінформована про своє право звернутися зі скаргою до Уповноваженого;

2) стаття 33 Постанови 45/2001 передбачає право будь-якої особи, найнятої на роботу установою або органом ЄС, подати скаргу Уповноваженому за наявності підозри щодо порушення норм Постанови, причому скарга може бути подана в обхід офіційних каналів. При цьому ніхто не може бути підданий переслідуванню за подачу подібної скарги. Можна припустити, що у зв'язку з величезним

ISSN 1995-6134

обсягом обробки персональних даних, і особливо «чутливих даних», наприклад про медичний стан суб'єктів даних, їх релігійних переконання або членство в професійних спілках, дана категорія скарг може складати значний обсяг роботи апарату Уповноваженого.

Згідно зі ст.46 (b) Постанови 45/2001, Уповноважений з власної ініціативи або на підставі скарги уповноважений направляти запити та інформувати суб'єкта даних про результати запиту в межах розумного періоду часу. Тривалість розумного періоду часу не уточнюється. Регламент 45/2001 наділив Уповноваженого достатніми повноваженнями, що сприяють збору необхідної інформації для проведення розслідування за скаргою. Зокрема, Уповноважений має право вимагати від контролера даних (згідно ст.2 (d) Регламенту 45/2001 під Контролером даних розуміється будь-яка установа або орган ЄС, структурний підрозділ, який самостійно або спільно визначає цілі та способи обробки персональних даних), або від установи ЄС відкриття доступу до будь-яких персональних даних і до будь-якої інформації, що стосується запиту, а також доступу до всіх приміщень, де контролер даних або орган ЄС здійснюють свою діяльність (у випадку, коли є достатні підстави вважати, що діяльність, яка підпадає під сферу застосування Постанови 45/2001, здійснюється саме там) [3].

Даному повноваженню кореспондує обов'язок контролерів даних співпрацювати та сприяти Уповноваженому у здійсненні його діяльності, особливо за допомогою надання необхідної інформації та доступу. В результаті свого запиту та розслідування Уповноважений може дійти висновку про можливе порушення права на захист персональних даних. У цьому випадку він може надавати допомогу суб'єктам з приводу здійснення ними своїх прав; вжити заходів щодо контролера даних у разі наявності підозри на порушення положень із захисту персональних даних та внести пропозиції щодо захисту порушених прав. А також, протягом розумного періоду часу контролер повинен повідомити Уповноваженого про його наміри щодо виправлення ситуації та вжиті заходи щодо усунення зауважень Уповноваженого. Крім того, Уповноважений може винести зауваження або попередження контролеру даних, вимагати виправлення, блокування, стирання чи знищення даних у разі їх обробки в порушення норм Постанови та вимагати аналогічних дій від третіх осіб, яким дані розкривалися, або виставити тимчасову або остаточну заборона на обробку даних. Уповноважений також має право передати справу на розгляд вищих органів ЄС, Суду Європейських співтовариств і брати участь в судовому розгляді [3].

Діяльність Уповноваженого носить характер взаємодії, що здійснюється в двох основних площинах – у площині національних органів влади (обмін інформацією, вимога виконання своїх зобов'язань із захисту інформації та розгляд спірних питань) і в площині наглядових органів ЄС (співробітництво з Європолом, органами Шенгенської угоди та Eurojust) [4, с.34].

Істотні повноваження надані Уповноваженому в частині застосування «винятків із правил». Це одна з ключових функцій даної уповноваженої особи, яка надає правову систему захисту персональних даних певну гнучкість, необхідну для адаптації Постанови до ситуацій, які не могли бути передбачені законодавцями при підготовці даного документа. При цьому Уповноважений виступає гарантом дотримання прав суб'єктів даних, що накладає на нього додаткову відповідальність. Зокрема, ст.10 Постанови 45/2001 забороняє обробку «чутливих даних» – даних про расову приналежність та релігійне віросповідання, про здоров'я чи членство в громадських організаціях [3]. Тим не менш, обробка подібних даних може бути проведена за умови дотримання наступних умов:

1) обробка даних необхідна при виконанні контролером даних функцій роботодавця щодо найманих працівників відповідно до законодавства ЄС та Договору про ЄС;

2) обробка даних здійснюється за схвалення Уповноваженого.

При наявності певних правових і технічних гарантій Уповноважений має право санкціо-

ISSN 1995-6134

нувати обробку особистих даних у статистичних цілях або у випадку, коли це необхідно в інтересах історичного чи наукового дослідження, причому без інформування суб'єктів даних про цілі та способи обробки даних про них, як це передбачено практично у всіх інших випадках обробки персональних даних. Уповноважений також може схвалити обробку даних про телефонні розмови – дані трафіку – для цілей планування телекомунікаційного бюджету передавальної компанії або для цілей управління трафіком.

Слідуючи за Директивою ЄС 95/46/ЄС про захист фізичних осіб щодо обробки персональних даних і вільне пересування персональних даних, Регламент 45/2001 встановив правило про обов'язкове повідомлення контролерами даних про операції з обробки персональних даних. Відповідно до статті 24 документа, кожен орган ЄС призначає спеціально уповноважену особу – Офіцера із захисту персональних даних, завданнями якого є забезпечення суб'єктів даних інформацією про їхні права, дотримання норм Постанови 45/2001 на конкретному інституційному рівні, сприяння Уповноваженому у розслідуванні скарг, повідомлення останнього про ризиковані операції з обробки даних (офіцери із захисту персональних даних вже працюють в Європейському Парламенті, Раді Європейського Союзу, Європейської Комісії, Європейському Суді Правосуддя, Суді Аудиторів, Європейському економічному та соціальному комітеті, Комітеті Регіонів, Європейських Центральному та Інвестиційному Банках, в апараті Уповноваженого з прав людини, Антикорупційному відомстві, Центрі перекладів для установ ЄС, Офісі з гармонізації внутрішнього ринку, Європейському центрі з моніторингу расизму та ксенофобії, Європейському медичному агентстві) [5, с.43].

Офіцер також виконує й функцію реєстратора операцій з обробки даних, саме його контролери повинні завчасно повідомляти про подібні операції. Так, офіцер повинен бути проінформований про найменування контролера та орган, уповноваживши його на проведення операцій, метою обробки, про категорії суб'єктів даних, правові підстави обробки, про категорії одержувачів інформації тощо. Уповноважений має право прямо або побічно перевіряти реєстри операцій.

На думку європейських законодавців, обробка даних про здоров'я громадян, про підозру у скоєнні злочину, про наявність звинувачень та застосування запобіжних заходів, а також здійснення операцій, спрямованих на оцінку здібностей, поведінки громадян або на обмеження їх прав, у тому числі за договором, являє собою певний загрозу захисту прав і свобод громадян за своєю природою або в силу цілей обробки даних. Усі подібні операції підлягають попередній перевірці Уповноваженим з повідомленням Офіцера із захисту даних [6, с.101].

Рішення має бути прийнято протягом двох місяців, а в особливо складних випадках – протягом чотирьох. У разі неподання відповіді в термін вважається, що рішення сприятливе з точки зору здійснення операції з обробки даних. У своєму рішенні Уповноважений може також вказати на потенційну можливість порушення норм Регламенту 45/2001, при цьому, де це потрібно, повинен бути зазначений спосіб уникнути порушення законодавства. Всю повноту своїх повноважень, аж до вимоги знищення даних або передачі справи до Суду Європейських співтовариств, в якому Уповноважений може бути позивачем, відповідачем, стороною у справі, Уповноважений може застосувати у разі невиконання контролером даних вказівок Уповноваженого згідно проведеної попередньої перевірки.

Європейське законодавство про захист персональних даних накладає суттєві обмеження на передачу даних у треті країни, де не існує адекватного режиму їх захисту. Винятки можливі у випадку, якщо, наприклад, передача даних необхідна для захисту життєво важливих інтересів суб'єкта або коли суб'єкт сам дав на це свою згоду. Однак Уповноважений може схвалити передачу даних у треті країни або інші міжнародні організації, якщо визнає, що рівень захисту даних, а отже, і прав їхніх суб'єктів відповідає необхідним правовим параметрам. Адекватність захисту може ви-

ISSN 1995-6134

пливати із зобов'язань, прийнятих, наприклад, на основі двох-і багатосторонніх угод і договорів про захист персональних даних.

Виходячи з загальних вимог міжнародних стандартів і законодавчої практики країн Європи, зокрема, ст.13 Конвенції № 108 Ради Європи, перелік першочергово необхідних нормативно-організаційних актів для ефективного функціонування системи захисту персональних даних в Україні передбачає обов'язкову наявність наступних нормативних документів: 1) положення про Уповноважений орган з питань захисту персональних даних; 2) положення про надання дозволу на здійснення діяльності у сфері захисту персональних даних; 3) положення про реєстрацію баз персональних даних, систем автоматизованої обробки і систем обробки картотек персональних даних.

Разом із тим, належний та повноцінний захист персональних даних у різних органах державної влади, організаціях, установах, підприємствах, а також ефективна робота Уповноваженого органу просто неможливі без ряду інших підзаконних нормативно-організаційних актів, які покликані конкретизувати окремі напрямки захисту персональних даних. До таких документів, зокрема, слід віднести також акт, що визначає роботу Уповноваженого організації (фірми) із захисту персональних даних [7, с.121].

Спираючись на європейську практику країн, де вже не один рік функціонують цільові закони та сформований відповідний правовий механізм захисту персональних даних, спробуємо проаналізувати чинні нормативно-правові акти України у сфері захисту персональних даних.

Так, зокрема, Указом Президента України «Про затвердження Положення про Державну службу України з питань захисту персональних даних» від 06.04.2011 р. (далі – Положення) [8] визначено уповноваженим державним органом з питань захисту персональних даних – Державну службу України з питань захисту персональних даних, одним із основних завдань якої є реєстрація баз персональних даних. Згідно цього Положення Державна служба України з питань захисту персональних даних (далі – ДСЗПД України) є центральним органом виконавчої влади, діяльність якої спрямовується і координується Кабінетом Міністрів України через Міністра юстиції України. ДСЗПД України входить до системи органів виконавчої влади, забезпечує реалізацію державної політики у сфері захисту персональних даних. Дана норм цілком відповідає положенню ст.23 Закону України «Про захист персональних даних»: «Уповноважений державний орган з питань захисту персональних даних – центральний орган виконавчої влади, до повноважень якого належить захист персональних даних, що утворюється відповідно до законодавства» [1].

На перший погляд це відповідає європейському досвіду, де існує інститут Уповноваженого з питань захисту персональних даних. Однак, на відміну від України, Уповноважений є незалежною структурою (яка хоча й може призначатися владними органами), що забезпечує баланс особистих, громадських та державних інтересів [9].

Крім того, згідно положень ст.28 Директиви 95/46/ЄС Європарламенту та Ради Євросоюзу від 24.10.1995 р. про захист прав приватних осіб щодо обробки персональних даних і про вільний рух таких даних, відповідний державний орган обов'язково повинен діяти в умовах повної незалежності та складати регулярні звіти про свою діяльність, які підлягають опублікуванню.

Натомість, у нашому законодавстві немає жодних положень про незалежність уповноваженого органу, що може унеможливити забезпечення захисту інтересів громадянина від можливих неправомірних дій (в тому числі і з боку держави).

Досвід ряду європейських країн свідчить також і про те, що Уповноважений орган з питань захисту персональних даних – це структура, що підпорядковується парламенту, тобто, це організаційна структура, що має спеціальні повноваження, які визначені саме парламентом, що здійснює нагляд і контроль діяльності у сфері захисту персональних даних, несе відповідальність за вирішення питань щодо виконання законодавства про захист персональних даних. Наведемо декілька прикладів:

ISSN 1995-6134

Австрія: Спочатку передбачалося запровадження посади Омбудсмена з питань недоторканності приватного життя, проте після п'ятирічних дебатів Закон «Про захист даних» 1978 р. встановив подвійну регулюючу структуру, що складається з Ради із захисту даних та Комісії із захисту даних [10].

Бельгія: Законодавчий акт 1992 р. про захист даних засновує спеціальний незалежний орган влади – Комісію із захисту недоторканності приватного життя, який відповідальний за забезпечення «добросовісної практики щодо файлів даних» [11].

Великобританія: Об'єднане Королівство не має власного тексту конституції. В 1998 р. британський парламент затвердив Акт про права людини, що надає Європейської конвенції з прав людини силу національного закону; цей процес повинен був завершитися законодавчим закріпленням права на недоторканність приватного життя. Акт набрав чинності в жовтні 2000 р. У липні 1998 р. парламент прийняв Закон про захист інформації, що приводить аналогічний Закон 1984 р. у відповідність до вимог Директиви про захист інформації, прийнятої Європейським Союзом. Дія закону поширюється на облікові записи, що ведуться державними установами та приватними компаніями. Він накладає ряд обмежень на використання персональних даних та на доступ до облікових записів, а також зобов'язує юридичні особи, які ведуть такі записи, реєструватися в Комісаріаті із захисту інформації. Комісаріат із захисту інформації є незалежним агентством, що забезпечує дотримання вимог закону [12].

Німеччина: Інститут Уповноваженого з питань захисту персональних даних почав формуватися у 1970 р., коли в Землі Гессен вперше у світі був прийнятий цільовий Закон «Про захист даних». Закон установив державну посаду Комісара по захисту даних на правах єдиноначальності. Цьому виборному державному службовцю Закон надав і забезпечив право повної незалежності від владних структур (жоден орган виконавчої влади не може давати йому вказівки), а також – надав право спостереження за діяльністю щодо персональних даних. Як наглядова, незалежна інстанція Комісар не несе прямої відповідальності за обробку персональних даних [13].

Таким чином, зробимо наступні висновки. Український досвід створення спеціальної інституційної структури, що здійснює контроль над законністю операцій з персональними даними, і здійснює захист прав їх суб'єктів, багато в чому схожий з європейським. Слідуючи європейським традиціям, Закон України «Про захист персональних даних» докладно розкрив компетенцію Уповноваженого органу, надавши йому сукупність досить ефективних засобів впливу на порушників законодавства про персональні дані, контролю діяльності суб'єктів, що здійснюють їх обробку, а також захисту прав суб'єктів відповідної інформації.

Основний критичною характеристикою статусу Уповноваженого органу, що виділяється теоретиками права, є його «залежність» від інших владних структур у силу його входження в систему органів виконавчої влади України. Досвід європейських країн свідчить про те, що Уповноважений орган з питань захисту персональних даних – це є структура, що підпорядковується парламенту, тобто, це організаційна структура, що має спеціальні повноваження, які визначені саме парламентом, що здійснює нагляд і контроль діяльності у сфері захисту персональних даних, несе відповідальність за вирішення питань щодо виконання законодавства про захист персональних даних.

ЛІТЕРАТУРА

1. Закон України «Про захист персональних даних» : від 01.06.2010 р. – К. : Парлам. вид-во, 2010. – 34 с.

2. Вельдер И. А. Система правовой защиты персональных данных в Европейском Союзе: дис. ... кандидата юрид. наук : 12.00.10 / Вельдер Илья Александрович. – Казань, 2006. – 164 с.

3. Про захист прав приватних осіб щодо обробки персональних даних органами та установами ЄС та про вільний рух таких даних : регламент Європейського парламенту та Ради : від 18.12.2000 р., № 45/2001 // Інформаційне законодавство : зб. законодавчих актів : у 6 т. Т. 5. Міжнародно-правові акти в інформацій-

ISSN 1995-6134

ній сфері / за заг.ред. Ю. С. Шемшученка, І. С. Чижа. – К. : Вид-во «Юрид. думка», 2005. – 328 с.

4. Валеев Р. М. Контроль в современном международном праве / Р. М. Валеев. – Казань : Центр инновац. технологий, 2001. – 211 с

5. Капустин А. Я. Европейский Союз: интеграция и право / А. Я. Капустин. – М. : Изд-во РУДН. – 2000. – 436 с.

6. Кашкин С. Ю. Право Европейского Союза / С. Ю. Кашкин. – М. : Проспект, 2005. – 331 с.

7. Брижко В. М. Організаційно-правові питання захисту персональних даних: дис. … кандидата юрид. наук : 12.00.07 / Брижко Валерій Михайлович. – К., 2004. – 203 с.

8. Указ Президента України «Про затвердження Положення про Державну службу України з питань захисту персональних даних» : від 06.04.2011 р. // Офіційний вісник України. – 2011. – № 28. – Ст. 1160.

9. Оніщенко І. Захист персональних даних «по новому» – крок в Європу чи навпаки / І. Оніщенко [Електронний ресурс]. – Режим доступу: http://news.ligazakon.ua/news/2011/1/17/36298.htm.

10. Захист персональних даних в Австрії [Електронний ресурс]. – Режим доступу: http://www.uipdp.com/solutions/services/consulting/legislation/eu/austria.html.

11. Захист персональних даних в Бельгії [Електронний ресурс]. – Режим доступу: http://www.uipdp.com/solutions/services/consulting/legislation/eu/belgium.html.

12. Захист персональних даних в Великобританії [Електронний ресурс]. – Режим доступу: http://www.uipdp.com/solutions/services/consulting/legislation/eu/england.html.

13. Захист персональних даних Німеччини [Електронний ресурс]. – Режим доступу: http://www.uipdp.com/solutions/services/consulting/legislation/eu/germany.html.

Різак М. В. Правовий статус уповноваженого органу з питань захисту персональних даних: досвід зарубіжних країн / М. В. Різак // Форум права. – 2012. – № 3. – С. 619–625 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2012-3/12rmvdzk.pdf

Висвітлено окремі особливості організації та діяльності уповноваженого органу з питань захисту персональних даних. Здійснено порівняльно-правовий аналіз контролю над відповідністю процесів збору, використання та розпорядження персональними даними, що здійснюються як на рівні державних (муніципальних), так і приватних структур, вимогам законодавства. Наводиться приклад зарубіжних країн, зокрема: Бельгії, Великобританії, Німеччини та Австрії.

***

Ризак М.В. Правовой статус уполномоченного органа по вопросам защиты персональных данных: опыт зарубежных стран

Освещены отдельные особенности организации и деятельности уполномоченного органа по вопросам защиты персональных данных. Осуществлен сравнительно-правовой анализ контроля за соответствием процессов сбора, использования и распоряжения персональными данными, совершаемые как на уровне государственных (муниципальных), так и частных структур, требованиям законодательства. Приводится пример зарубежных стран, в частности: Бельгии, Великобритании, Германии и Австрии.

***

Rizak M.V. Legal Status of Authorized Body Concerning Personal Data Protection: Experience of Foreign Countries

Some features of the organization and activities of the competent authority on the protection of personal data highlights. The article by comparative legal analysis of matched control of the collection, use, and disposal of personal data carried out at the level of government (municipal) and private structures, legal requirements. An example of other countries, including: Belgium, Britain, Germany and Austria.