УДК 347.1

Старчук Євген Валерійович
аспірант кафедри права
ПВНЗ «Європейський університет»
Starchuk Yevhen
Postgraduate Student of the
PHEI "European University"
ORCID: 0009-0000-3022-9349

DOI: 10.25313/2520-2308-2025-10-11531

ПЕРСПЕКТИВИ СТВОРЕННЯ НАЦІОНАЛЬНОГО ОРГАНУ ІЗ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

PROSPECTS FOR ESTABLISHING A NATIONAL PERSONAL DATA PROTECTION AUTHORITY IN UKRAINE

Анотація. *Вступ. У сучасному цифровому середовищі, де обробка персональних даних стала невід'ємною частиною державного управління, бізнесу та повсякденного життя громадян, питання їх захисту набуває особливої актуальності. В умовах війни, стрімкої цифровізації державних послуг, розвитку електронних реєстрів та мобільних додатків, обсяг і чутливість персональних даних, які збираються та обробляються, зростають у геометричній прогресії. Це створює нові ризики витоку, зловживань, несанкціонованого доступу та порушення приватності, які потребують системного та ефективного регулювання.*

Мета. Метою статті є аналіз правових передумов та обґрунтування необхідності створення Національної комісії з питань захисту персональних даних в Україні як спеціалізованого органу, здатного забезпечити ефективне регулювання та контроль у сфері цифрових прав, як аналога національних органів захисту даних, які діють в країнах ЄС.

Матеріали і методи. У процесі дослідження використано нормативно-правові акти України, положення Загального регламенту ЄС про захист даних (GDPR), Конвенції Ради Європи 108, а також аналітичні висновки профільних інституцій. Методологічну основу становлять загальнонаукові методи – аналіз, синтез, індукція, дедукція – та спеціально-юридичні методи: формально-юридичний, порівняльно-правовий, системний аналіз. Застосовано емпіричне дослідження практики функціонування органів захисту персональних даних у країнах ЄС, США та Канаді з метою виявлення оптимальної моделі для України.

Результати. У результаті дослідження встановлено, що чинна модель захисту персональних даних в Україні, представлена інститутом Уповноваженого Верховної Ради з прав людини, є недостатньо ефективною через обмеженість повноважень та ресурсів. Аналіз законопроєкту № 6177 свідчить про намір створити спеціалізований орган – Національну комісію з питань захисту персональних даних, який матиме розширені контрольні, регуляторні та санкційні функції. Виявлено, що запропонована модель відповідає європейським стандартам, зокрема вимогам GDPR та Конвенції 108, і має потенціал забезпечити системний та незалежний нагляд у сфері цифрових прав. Разом з тим, окремі положення законопроєкту викликають занепокоєння щодо можливих корупційних ризиків, що потребує додаткового нормативного уточнення.

Перспективи. Створення Національної комісії з питань захисту персональних даних відкриває широкі можливості для формування ефективної системи цифрового регулювання в Україні. Комісія може стати дієвим інструментом захисту прав громадян у цифровому середовищі, сприяти прозорості обробки персональних даних, підвищенню довіри до державних та приватних інституцій. Водночас, для мінімізації ризиків зловживань необхідне чітке нормативне врегулювання процедур контролю, санкцій та забезпечення незалежності органу.

Ключові слова: *персональні дані, цифрові права, Національна комісія, GDPR, захист інформації, законопроєкт № 6177, державний контроль, євроінтеграція, приватність, регуляторний орган.*

Summary. *Introduction. In the modern digital environment, where the processing of personal data has become an integral part of public administration, business, and everyday life, the issue of data protection is gaining particular relevance. In the context of war, rapid digitalization of public services, development of electronic registries and mobile applications, the volume and sensitivity of personal data being collected and processed are growing exponentially. This creates new risks of data leakage, abuse, unauthorized access, and privacy violations, which require systematic and effective regulation.*

Purpose. The purpose of this article is to analyze the legal prerequisites and justify the need to establish a National Personal Data Protection Commission in Ukraine as a specialized body capable of ensuring effective regulation and oversight in the field of digital rights, similar to national data protection authorities operating in EU countries.

Materials and Methods. The study uses Ukrainian legal acts, provisions of the EU General Data Protection Regulation (GDPR), the Council of Europe Convention 108, as well as analytical conclusions of relevant institutions. The methodological basis includes general scientific methods – analysis, synthesis, induction, deduction – and special legal methods: formal legal, comparative legal, and system analysis. Empirical research of the functioning of data protection authorities in the EU, USA, and Canada was conducted to identify the optimal model for Ukraine.

Results. The study found that the current model of personal data protection in Ukraine, represented by the institution of the Parliamentary Commissioner for Human Rights, is insufficiently effective due to limited powers and resources. Analysis of draft law No. 6177 indicates the intention to create a specialized body – the National Personal Data Protection Commission – with expanded control, regulatory, and sanctioning functions. The proposed model aligns with European standards, particularly the GDPR and Convention 108, and has the potential to ensure systematic and independent oversight in the field of digital rights. However, certain provisions of the draft law raise concerns about potential corruption risks, which require further regulatory clarification.

Discussion. The establishment of the National Personal Data Protection Commission opens up broad opportunities for forming an effective digital regulation system in Ukraine. The Commission could become a powerful tool for protecting citizens' rights in the digital environment, promoting transparency in personal data processing, and increasing trust in public and private institutions. At the same time, to minimize risks of abuse, clear regulatory procedures for oversight, sanctions, and ensuring the independence of the body are necessary.

Key words: *personal data, digital rights, National Commission, GDPR, data protection, draft law No. 6177, state oversight, European integration, privacy, regulatory authority.*

Постановка проблеми. Після набуття чинності Загального регламенту ЄС про захист даних (GDPR) [1] у травні 2018 року, кожна держава-член Європейського Союзу зобов'язана створити незалежний орган, відповідальних за моніторинг дотримання положень Регламенту (ст. 51 GDPR). На сьогодні, у більшості європейських країн національні органи захисту персональних даних функціонують вже багато років, забезпечуючи ефективний контроль, накладення санкцій, сертифікацію, перевірки та розслідування порушень.

В Україні ж спеціалізований орган — Державна служба з питань захисту персональних даних — існував лише три роки, після чого його функції були передані Уповноваженому Верховної Ради з прав людини. Однак, така модель не забезпечує належного рівня захисту, оскільки інститут Уповноваженого не має достатніх ресурсів, повноважень та інструментів для системного контролю, і створений для вирішення зовсім інших завдань.

Важливою проблемою є вирішення питань контролю за цивільним обігом інформації у вигляді персональних даних (баз чи окремих даних фізичних осіб), яка на сьогодні залишається поза увагою профільних органів.

У зв'язку з цим актуальним є дослідження правової природи, функцій та повноважень національних органів захисту персональних даних, а також обґрунтування необхідності створення в Україні незалежного адміністративного органу, здатного забезпечити належний рівень захисту персональних даних відповідно до європейських стандартів.

Аналіз останніх досліджень та публікацій. Окремі аспекти правового забезпечення захисту персональних даних досліджувалися низкою українських вчених. Так, О. Тимошенко розглядає правове забезпечення захисту персональних даних в Україні, з урахуванням практики Європейського суду з прав людини [2]. Р. Пристай досліджує специфіку захисту персональних даних в соціальних мережах [3]. А. Гачкевич вивчає питання нагляду національних органів за обробкою персональних даних системи штучного інтелекту [4]. Також питання захисту персональних даних досліджували К. Мельник [5], Тейлор Г., Школьний Є.

Мета статті. Метою статті є аналіз правових передумов та обґрунтування необхідності створення Національної комісії з питань захисту персональних даних в Україні як спеціалізованого органу, здатного забезпечити ефективне регулювання та контроль у сфері цифрових прав, як аналога національних органів захисту даних, які діють в країнах ЄС.

Виклад основного матеріалу. Питання створення в Україні національного органу з захисту персональних даних стало актуальним у контексті євроінтеграційних процесів, зростання цифрових викликів і необхідності гармонізації національного законодавства з європейськими стандартами. Угода про асоціацію між Україною та Європейським Союзом (2014) [6], зокрема її ст. 14–15, зобов'язує

Україну привести законодавство у сфері захисту даних у відповідність до європейського. Ключовим елементом такої гармонізації є створення незалежного наглядового органу, подібного до національних органів захисту даних (Data Protection Authorities, DPAs) країн ЄС, які відповідають за моніторинг і виконання норм GDPR. Крім того, отримання Україною статусу кандидата на вступ до ЄС у 2022 році посилило необхідність інституційних реформ у цій сфері, зокрема через вимоги до імплементації європейських стандартів захисту даних.

Одним із основних стимулів для запровадження окремого органу є недостатня ефективність чинної системи нагляду за захистом персональних даних в Україні. Наразі ці функції виконує Уповноважений Верховної Ради України з прав людини (Омбудсман) відповідно до Закону України «Про захист персональних даних» [7]. Однак ця інституція не відповідає стандартам незалежності, визначеним GDPR (ст. 52), оскільки поєднує широкий спектр повноважень із захисту прав людини, що ускладнює спеціалізований нагляд за обробкою даних. Крім того, Омбудсман має обмежені ресурси, експертизу та повноваження, зокрема щодо накладання штрафів чи проведення розслідувань, які є стандартною практикою для DPAs в ЄС. Політична залежність, пов'язана з призначенням Омбудсмана парламентом, також викликає сумніви щодо відповідності європейським вимогам.

Зростання цифрових технологій і кіберзагроз стало ще одним фактором, що актуалізує потребу в спеціалізованому органі. Розвиток цифрових сервісів, таких як платформа «Дія», використання штучного інтелекту, хмарних технологій і обробка великих масивів даних (Big Data) підвищують ризики порушення прав на приватність. Кібератаки, спрямовані на персональні дані, стали регулярними, що вимагає швидкого реагування та координації з міжнародними партнерами. Окремий орган із захисту даних міг би ефективно виконувати функції розслідування, сертифікації та співпраці з Європейською радою із захисту даних (EDPB), зокрема в контексті транскордонної передачі даних, яка є критичною для співпраці з компаніями ЄС.

Суспільний запит на захист приватності також відіграє важливу роль у формуванні дискусії щодо створення нового органу. Громадяни України дедалі частіше стикаються з порушеннями у сфері обробки персональних даних державними органами, медичними установами чи приватними компаніями. Водночас чинне законодавство не передбачає ефективних механізмів захисту, таких як значні штрафи, передбачені GDPR (до 20 млн. євро або 4% річного обороту компаній, ст. 83). Створення спеціалізованого органу дозволило б запровадити такі інструменти, а також забезпечити розгляд скарг громадян і судовий захист їхніх прав. Досвід країн ЄС, де діють незалежні DPAs (наприклад, Garante в Італії, CNIL у Франції), демонструє ефективність такої моделі.

Міжнародний досвід і рекомендації також впливають на необхідність реформування системи захисту даних в Україні. Рішення Суду ЄС у справах C-518/07 (Комісія проти Німеччини, 2010) [8] та C-614/10 (Комісія проти Австрії, 2012) [9] підкреслили важливість незалежності наглядових органів, що стало орієнтиром для України. Рада Європи, зокрема через модернізовану Конвенцію 108 [10], рекомендує створення спеціалізованих інституцій для забезпечення захисту даних. Програми підтримки ЄС, такі як EU4Digital і проєкти Twinning, також стимулюють Україну до створення окремого органу для координації з європейськими партнерами та виконання міжнародних зобов'язань.

Саме тому в Україні було розроблено законопроєкт № 6177 [11], який передбачає створення Національної комісії з питань захисту персональних даних та доступу до публічної інформації. Цей орган має стати центральним органом виконавчої влади зі спеціальним статусом, наділеним широкими повноваженнями: від нормативного регулювання до контролю, перевірок, розгляду скарг та накладення санкцій. Комісія матиме право видавати рішення, що прирівнюються до виконавчих документів, здійснювати планові та позапланові перевірки, а також надавати методичну допомогу суб'єктам, які обробляють персональні дані.

Майбутня Комісія буде адміністративно-наглядовим органом, здатним забезпечити постійний моніторинг та регулювання у сфері захисту даних.

У більшості країн Європи вже діють незалежні органи — Data Protection Authorities (DPA), які забезпечують ефективний захист цифрових прав громадян. Аналогічні структури існують у США, Канаді, Великій Британії, Франції, Німеччині та інших країнах.

Європейський Союз

Національні органи захисту даних (Data Protection Authorities, DPA) — діють у кожній країні-члені ЄС.

Європейський наглядовий орган із захисту даних (EDPS) — контролює інституції ЄС.

США

Федеральна торгова комісія (FTC) — виконує частину функцій у сфері захисту приватності.

Канада

Office of the Privacy Commissioner of Canada — регулює захист персональних даних відповідно до закону PIPEDA (Personal Information Protection and Electronic Documents Act).

Створення Національної комісії дозволить Україні не лише виконати міжнародні зобов'язання, а й забезпечити реальний захист персональних даних своїх громадян на рівні, що відповідає сучасним викликам.

Комісія наділяється широкими повноваженнями, які охоплюють контрольні, регуляторні, консультативні та санкційні функції. Вона має право здійс-

нювати виїзні та безвиїзні, планові та позапланові перевірки суб'єктів контролю щодо дотримання законодавства про захист персональних даних та доступ до публічної інформації.

За результатами перевірок Комісія має право приймати обов'язкові для виконання рішення про запобігання та/або усунення порушень, а також притягати до відповідальності суб'єктів контролю, включаючи посадових осіб. Її рішення мають статус виконавчих документів, що підлягають примусовому виконанню без додаткового судового розгляду.

Окрім контрольних функцій, Комісія здійснює нормативну діяльність, зокрема погоджує проєкти нормативно-правових актів, які стосуються сфери її компетенції, та надає консультативні висновки Верховній Раді України щодо законопроєктів у сфері захисту персональних даних і доступу до інформації.

Також до її повноважень належать: надання роз'яснень, консультацій та методичних рекомендацій, моніторинг дотримання законодавства (п. 8 ч. 4 ст. 4), міжнародне співробітництво (п. 10 ч. 4 ст. 4), розробка рекомендацій програм навчання та підвищення кваліфікації, а також затвердження типового порядку здійснення відеоспостереження.

Ці повноваження забезпечують Комісії можливість діяти як незалежному регулятору, здатному ефективно реагувати на порушення, формувати політику у сфері захисту персональних даних та забезпечувати її реалізацію на практиці.

Процедура проведення перевірок Національною комісією з питань захисту персональних даних та доступу до публічної інформації, згідно з законопроєктом № 6177, має низку особливостей, які суттєво відрізняються від загальних правил державного нагляду.

Згідно з частиною 7 статті 46 законопроєкту, інспектори Комісії мають право проводити перевірки без спеціального рішення або направлення. Для початку перевірки достатньо пред'явити службове посвідчення інспектора або уповноваженого працівника Комісії. Після цього керівник групи, яка здійснює перевірку, складає довідку про початок перевірки, форма якої затверджується Комісією. Ця довідка надається суб'єкту контролю при першій комунікації.

Згода суб'єкта контролю на перевірку не є обов'язковою, як і присутність його керівника або уповноваженої особи, за винятком випадків, коли перевірка проводиться за місцем фактичного провадження діяльності, якщо це місце є житлом.

Частина 3 статті 46 передбачає, що інформація про дату проведення планової перевірки не підлягає завчасному оприлюдненню, що створює умови для раптового контролю.

Тривалість перевірки встановлюється до 180 днів з моменту її початку (ч. 10 ст. 46), і може бути продовжена на розсуд Комісії, якщо суб'єкт контролю не співпрацює (ч. 11 ст. 46).

У разі відмови суб'єкта контролю або його посадових осіб допустити інспекторів до перевірки, передбачено накладення штрафу згідно з ч. 2 ст. 44. Розмір штрафу для юридичних осіб становить від 0,5% до 1% річного обороту, але не менше 3000 неоподаткованих мінімумів доходів громадян.

Ці положення свідчать про високий рівень дискреції, наданий Комісії, що викликає занепокоєння щодо можливих корупційних ризиків [12]. Зокрема, відсутність чітких критеріїв для визначення строків перевірки та розміру санкцій може створити умови для зловживань.

Висновки та перспективи подальших досліджень. У ході дослідження встановлено, що чинна модель захисту персональних даних в Україні є недостатньо ефективною та не відповідає сучасним викликам цифрового середовища. Передача відповідних повноважень Уповноваженому Верховної Ради з прав людини не забезпечує належного рівня контролю, оперативного реагування та санкційного впливу. Аналіз законопроєкту № 6177 свідчить про прагнення держави створити спеціалізований орган — Національну комісію з питань захисту персональних даних, яка має потенціал стати ефективним регулятором у сфері цифрових прав.

Запропонована модель відповідає європейським стандартам, зокрема GDPR та Конвенції 108, і може сприяти гармонізації українського законодавства з правом ЄС. Водночас, окремі положення законопроєкту (в сфері проведення перевірок та накладення санкцій), потребують додаткового нормативного уточнення для запобігання корупційним ризикам та забезпечення прозорості діяльності Комісії.

Перспективи подальших досліджень полягають у:
– аналізі практики функціонування аналогічних органів у країнах ЄС;
– дослідженні механізмів контролю за обробкою персональних даних у соціальних мережах;
– розробці моделей взаємодії Національної комісії з іншими державними органами та громадянським суспільством;
– оцінці ефективності санкційних механізмів у сфері цифрових прав;
– вивченні правових аспектів захисту персональних даних у контексті використання штучного інтелекту.

Література

1. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент захисту даних).

2. Тимошенко О. А. Захист персональних даних в цивільних правовідносинах: вітчизняне правове забезпечення крізь призму практики Європейського суду з прав людини. *Актуальні проблеми правознавства*. 2023. № 4. URL: https://app-journal.in.ua/wp-content/uploads/2023/09/29.pdf (дата звернення: 27.10.2025).

3. Пристай Р. Національні органи захисту даних в Європейському Союзі: роль і практика в сфері захисту персональних даних в соціальних мережах. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 2, № 82. С. 245–252. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.39.

4. Гачкевич А. Нагляд національних органів ЄС із захисту даних за обробкою персональних даних системами штучного інтелекту (на прикладі ChatGPT). *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 2, № 4. С. 154–160. DOI: https://doi.org/10.24144/2788-6018.2025.04.2.24.

5. Мельник К. С. Теоретичні та організаційно-правові засади захисту персональних даних в контексті євроінтеграції України: монографія. Київ : ТОВ «ПанТот», 2016. 126 с.

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 27 червня 2014 року. Офіційний вісник України. 2014. № 75. Ст. 2125. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 27.10.2025).

7. Про захист персональних даних : Закон України від 1 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 435. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 27.10.2025).

8. Рішення Суду Європейського Союзу у справі C-518/07, Європейська Комісія проти Федеративної Республіки Німеччина, від 9 березня 2010 року. European Court Reports 2010, I-01885. URL: https://curia.europa.eu/juris/liste.jsf?num=C-518/07 (дата звернення: 27.10.2025).

9. Рішення Суду Європейського Союзу у справі C-614/10, Європейська Комісія проти Республіки Австрія, від 16 жовтня 2012 року. European Court Reports 2012, I-0000. URL: https://curia.europa.eu/juris/liste.jsf?num=C-614/10 (дата звернення: 27.10.2025).

10. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108) від 28 січня 1981 року. Офіційний вісник України. 2010. № 87. Ст. 2946. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 27.10.2025).

11. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації : Проєкт Закону України від 18 жовтня 2021 р. № 6177. URL: https://itdata.rada.gov.ua/bills/text/72992?lang=uk (дата звернення: 27.10.2025).

12. Висновок щодо законопроекту № 6177 «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації». *Інститут законодавчих ідей.* Київ : ІЗІ, 2021. URL: https://rge9.izi.institute/conclusion/pro-natsionalnu-komisiyu-z-pytan-zahystu-personalnyh-danyh-ta-dostupu-do-publichnoyi-informatsiyi/ (дата звернення: 27.10.2025).

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2. Tymoshenko, O. A. (2023). *Zakhyst personal'nykh danykh v tsyvil'nykh pravovidnosynakh: vitchyzniane pravove zabezpechennia kriz' pryzmu praktyky Yevropeis'koho sudu z prav liudyny* [Protection of personal data in civil legal relations: national legal framework through the lens of ECtHR practice]. *Aktual'ni problemy pravoznavstva*, (4). Retrieved from https://app-journal.in.ua/wp-content/uploads/2023/09/29.pdf

3. Prystai, R. (2024). *Natsional'ni orhany zakhystu danykh v Yevropeis'komu Soiuzi: rol' i praktyka v sferi zakhystu personal'nykh danykh v sotsial'nykh merezhakh* [National data protection authorities in the EU: role and practice in the field of personal data protection in social networks]. *Naukovyi visnyk Uzhhorods'koho natsional'noho universytetu. Seriia: Pravo*, 2(82), 245–252. https://doi.org/10.24144/2307-3322.2024.82.2.39

4. Hachkevych, A. (2024). *Nahlad natsional'nykh orhaniv YeS iz zakhystu danykh za obrobkoiu personal'nykh danykh systemamy shtuchnoho intelektu (na prykladi ChatGPT)* [Supervision by EU national data protection authorities over personal data processing by AI systems (case of ChatGPT)]. *Naukovyi visnyk Uzhhorods'koho natsional'noho universytetu. Seriia: Pravo*, 2(4), 154–160. https://doi.org/10.24144/2788–6018.2025.04.2.24

5. Mel′nyk, K. S. (2016). *Teoretychni ta orhanizatsiino-pravovi zasady zakhystu personal'nykh danykh v konteksti yevrointehratsii Ukrainy* [Theoretical and organizational-legal foundations of personal data protection in the context of Ukraine's European integration]. Kyiv: TOV "PanTot".

6. Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part, signed on 27 June 2014. *Ofitsiinyi visnyk Ukrainy*, 2014, No. 75, Art. 2125. https://zakon.rada.gov.ua/laws/show/984_011#Text

7. Zakon Ukrainy "Pro zakhyst personal'nykh danykh" vid 1 chervnia 2010 r. No. 2297-VI [Law of Ukraine "On Personal Data Protection" of June 1, 2010, No. 2297-VI]. *Vidomosti Verkhovnoi Rady Ukrainy*, 2010, No. 34, Art. 435. https://zakon.rada.gov.ua/laws/show/2297-17#Text

8. Judgment of the Court of Justice of the European Union in Case C-518/07, European Commission v. Federal Republic of Germany, March 9, 2010. *European Court Reports*, 2010, I-01885. https://curia.europa.eu/juris/liste.jsf?num=C-518/07

9. Judgment of the Court of Justice of the European Union in Case C-614/10, European Commission v. Republic of Austria, October 16, 2012. *European Court Reports*, 2012, I-0000. https://curia.europa.eu/juris/liste.jsf?num=C-614/10

10. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Council of Europe, January 28, 1981. *Ofitsiinyi visnyk Ukrainy*, 2010, No. 87, Art. 2946. https://zakon.rada.gov.ua/laws/show/994_326#Text

11. Draft Law of Ukraine "On the National Commission for Personal Data Protection and Access to Public Information" of October 18, 2021, No. 6177. https://itdata.rada.gov.ua/bills/text/72992?lang=uk

12. Conclusion on Draft Law No. 6177 "On the National Commission for Personal Data Protection and Access to Public Information". Institute of Legislative Ideas. Kyiv: IZI, 2021. https://rge9.izi.institute/conclusion/pro-natsionalnu-komisiyu-z-pytan-zahystu-personalnyh-danyh-ta-dostupu-do-publichnoyi-informatsiyi/