УДК 342.1
DOI https://doi.org/10.24144/2307-3322.2024.83.2.25

ПРОЗОРІСТЬ ТА ЗГОДА ЯК ОСНОВНІ ПРИНЦИПИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Головацький Н.Т.,
старший викладач
кафедри адміністративного, фінансового
та інформаційного права
юридичного факультету
ДВНЗ «Ужгородський національний університет»

Головацький Н.Т. Прозорість та згода як основні принципи захисту персональних даних в Україні.

Стрімке оцифровування сучасного світу призвело до зростання збору та обробки персональних даних. Принципи прозорості та згоди стали вкрай важливими для того, щоб громадяни розуміли, як їхні дані використовуються, і могли дати свою добровільну згоду на їх обробку.

Україна активно адаптує своє законодавство до стандартів ЄС у сфері захисту персональних даних. Зокрема, Загальний регламент про захист даних (GDPR) впливає на підходи до збору та обробки даних. Дослідження прозорості та згоди в контексті цих змін може допомогти визначити, які аспекти законодавства потребують особливої уваги. Громадяни стають дедалі обережнішими щодо того, кому вони довіряють свої дані.

Ця стаття аналізує та оцінює роль та вплив принципів прозорості та згоди на ефективний механізм захисту персональних даних в Україні, з урахуванням сучасних технологічних та законодавчих викликів. Вивчення цих принципів демонструє їх важливість та актуальність у сучасному цифровому суспільстві.

Принцип прозорості визначає потребу в доступній та зрозумілій інформації для суб'єктів даних щодо обробки їхніх даних. Відкритість є фундаментальною вимогою для підтримки довіри між організаціями та громадянами. Надання можливості контролювати та регулювати свої дані дозволяє суб'єктам даних відігравати більш активну роль в обробці та використанні своїх персональних даних.

Принцип згоди, у свою чергу, підкреслює добровільний та інформований характер дозволу на обробку даних. Згода суб'єкта даних визначає основу для законної обробки персональних даних, забезпечуючи гармонію між правами громадян та інтересами організацій.

Зважаючи на розвиток технологій та зміни в законодавстві, прозорість та згода стають ще більш важливими аспектами. Вони допомагають збудувати довіру між організаціями та громадянами, забезпечити відповідальне використання персональних даних та надати можливість окремим особам контролювати свою власну інформацію.

Ключові слова: прозорість, згода, персональні дані, захист даних, законодавство, цифрове суспільство, технології, держава, громадяни, загальний регламент про захист даних (GDPR).

Holovatskiy N.T. Transparency and consent as the main principles of personal data protection in Ukraine.

The rapid digitization of the modern world has led to an increase in the collection and processing of personal data. The principles of transparency and consent have become crucial for citizens to understand how their data is being used and to be able to give their voluntary consent to its processing.

Ukraine is actively adapting its legislation to EU standards in the field of personal data protection. In particular, the General Data Protection Regulation (GDPR) affects approaches to data collection and processing. Examining transparency and consent in the context of these changes can help identify which aspects of the law need special attention. Citizens are becoming increasingly cautious about who they trust with their data.

This article analyzes and evaluates the role and impact of the principles of transparency and consent on the effective mechanism of personal data protection in Ukraine, taking into account modern technological and legislative challenges. Studying these principles demonstrates their importance and relevance in today's digital society.

The principle of transparency determines the need for accessible and understandable information for data subjects regarding the processing of their data. Openness is a fundamental requirement for maintaining trust between organizations and citizens. Providing the ability to control and regulate their data allows data subjects to play a more active role in the processing and use of their personal data.

The principle of consent, in turn, emphasizes the voluntary and informed nature of consent to data processing. The consent of the data subject determines the basis for the legal processing of personal data, ensuring harmony between the rights of citizens and the interests of organizations.

As technology advances and legislation changes, transparency and consent become even more important aspects. They help build trust between organizations and citizens, ensure responsible use of personal data, and empower individuals to control their own information.

Key words: transparency, consent, personal data, data protection, legislation, digital society, technology, state, citizens, General Data Protection Regulation (GDPR).

Постановка проблеми. Сучасний світ дедалі більше стає цифровим, із зростанням цифрових технологій збільшується обсяг збору та обробки персональних даних. Принципи прозорості та згоди стають ключовими для забезпечення того, щоб громадяни розуміли, як їхні дані використовуються, та давали свою добровільну згоду на обробку персональних даних. Чим більше дані збираються та обробляються, тим вище ризик незаконного доступу третіх осіб до таких даних. Прозорість щодо того, які дані збираються, і як вони обробляються, дозволяє громадянам краще розуміти можливі ризики та застереження.

Україна активно адаптує своє законодавство до стандартів ЄС з огляду на захист персональних даних. Зокрема, Загальний регламент про захист даних (GDPR) [1] має вплив на підходи до збору та обробки даних. Дослідження прозорості та згоди в контексті цих змін може допомогти визначити, які аспекти законодавства потребують особливої уваги.

Громадяни стають все більше обережнішими щодо того, кому вони довіряють свої дані. Прозорість відносно того, як дані використовуються, може сприяти зміцненню довіри до організацій та послуг, що збирають і обробляють дані.

Аналіз останніх досліджень і публікацій. Проблемам принципів захисту персональних даних у вітчизняній науці присвячено недостатньо наукових робіт.

Деякі питання означеної проблематики фрагментарно торкались у своїх працях такі науковці, як В.С. Венедіктов, А.М. Колодій, О.А. Баранов, В.М. Брижко, М.В. Різак, В.С. Політанський, Ю.К. Базанов, А.В. Пазюк, І.М. Сопілко, О.В. Старчук та інші. Проте, у наукових працях вказаних науковців питання принципів захисту персональних даних майже відсутні.

Мета статті. Проаналізувати та оцінити роль і вплив принципів прозорості та згоди на ефективний механізм захисту персональних даних в Україні із врахуванням сучасних технологічних та законодавчих викликів.

Виклад основного матеріалу. Захист персональних даних, як і будь яка юридична категорія, ґрунтується на певній системі принципів, завдяки яким такий механізм носить демократичний характер та стає соціально орієнтованим явищем. Дослідження питання щодо принципів захисту персональних даних надасть змогу визначити ідейно-правову сутність механізму захисту персональних даних в цілому.

Варто погодитись із думкою, В.М. Колодій, який зазначає, що принципи права – це ідеологічна категорія, а це означає, що вони, як і право загалом, є формою суспільної свідомості, яка здійснює ідейний, інформаційно-виховний вплив загального характеру, тобто виконує функцію загального закріплення суспільних відносин, що та дає можливість розглядати їх з позиції певних ідей, керівних засад [2, с. 43].

Термін «принцип» вживається у різних значеннях:

1) основні засади вихідні ідеї, що характеризуються універсальністю, загальною значущістю, вищою імперативністю і відображають суттєві положення теорії, вчення, науки, системи внутрішнього і міжнародного права, політичної, державної чи громадської організації (гуманізм, законність, справедливість, рівність громадян перед законом тощо);

2) внутрішнє переконання людини, що визначає її ставлення до дійсності, суспільних ідей і діяльності [3, с. 110-111].

Принципи права, як і будь-яке явище суспільної дійсності має конкретну точку відліку, з якої починається існування самого принципу права. В аспекті принципів права не можна стверджувати однозначно, що є первинним – суспільні відносини, на основі яких починають формуватися принципи права, чи принципи права, які є стимулятором розвитку нового виду суспільних відносин.

Стосовно цього О.В. Зайчук зазначає, що принципи права можуть формуватись через призму двох алгоритмів:

1) спочатку суспільні відносини, а потім принципи права;

2) спочатку принципи права, а потім на їх основі починають розвиватися суспільні відносини.

Перший алгоритм характеризує ситуацію коли на основі реальних суспільних відносин починають формуватися принципові закономірності їх функціонування, які отримують своє безпосереднє вираження у нормативному закріплені.

Стосовно другого алгоритму, то тут мова йде про те, що законодавець, фактично, закріплює новизну у вигляді принципу, яка потім отримує свою реалізацію в конкретних суспільних відносинах [4, с. 23].

Оцінюючи думки вказаних науковців слід відзначити той факт, що така ситуація замкнутого кола, є безпосередньою вказівкою низки прогалин законодавства, оскільки певні суспільні відносини не мають жорсткого законодавчого регулювання, а тому в конкретній ситуації спочатку є виникнення суспільних відносин, а потім формування принципу права.

Проте, якщо мова йде про захист персональних даних, а зокрема про принципи захисту персональних даних, то станом на сьогоднішній день, можна із впевненістю стверджувати, що діє саме другий алгоритм, оскільки принципи захисту персональних даних сформовані у вигляді прямої законодавчої норми та закріплені у статтях 6 і 7 Закону України «Про захист персональних даних» [5].

Стаття 6 Закону України «Про захист персональних даних» розкриває питання загальних вимог до обробки персональних даних. Стаття 7 цього ж Закону закріплює особливі вимоги. Аналізуючи Закон, варто відзначити, що законодавець не виділив окремо норму Закону в, якій були б зазначені виключно принципи збору, обробки та захисту персональних даних, а зробив це через призму вимог до персональних даних загалом. Таке рішення є цілком вмотивованим з точки зору того, що при виділенні окремої норми, яка закріплювала б принципи персональних даних, варто було б конкретизувати та закріплювати окремо принципи збору персональних даних, принципи обробки персональних даних, принципи захисту персональних даних, а також не менш важливого характеру принципи знищення персональних даних.

Статтею 6 «Загальні вимоги до обробки персональних даних» Закону України «Про захист персональних даних» передбачено:

– мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних;

– персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки;

– склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки;

– первинними джерелами відомостей про фізичну особу є: видані на її ім’я документи; підписані нею документи; відомості, які особа надає про себе.

– обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб’єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством;

– не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини;

– якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб’єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим;

– персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися;

– типовий порядок обробки персональних даних затверджується Уповноваженим Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних.

Виходячи з аналізу Закону України «Про захист персональних даних» ключовими принципами обробки персональних даних є: законність обробки; конкретизація мети; відкритість і прозорість обробки; якість даних: – відповідність даних меті обробки; – точність даних та вчасне оновлення даних; – достовірність даних; – обмеження періоду зберігання даних; – захищеність даних.

Отже, перш ніж розкривати принципи прозорості та згоди, як основних принципів захисту персональних даних, необхідно чітко розуміти принцип законності обробки персональних даних. Також варто відзначити, що принцип законності є основоположним принципом будь яких суспільних правовідносин.

Принцип законності захисту персональних даних є однією з фундаментальних засад, що регулюють обробку та використання особистих даних в Україні. Відповідно до цього принципу, обробка персональних даних повинна здійснюватися на підставі чіткої та визначеної законом підстави, з дотриманням вимог відповідних законів та нормативних актів.

Згідно з Законом України «Про захист персональних даних», обробка персональних даних може здійснюватися лише за наявності однієї з підстав, визначених законом. Ці підстави можуть включати згоду суб'єкта даних, виконання договору, дотримання законних обов'язків, захист важливих інтересів суб'єкта даних тощо. Тобто, кожна обробка персональних даних має мати законний підгрунтя, і цей принцип гарантує, що дані обробляються в рамках встановлених норм та процедур [5].

Цей принцип також передбачає, що організації та суб'єкти персональних даних повинні дотримуватися вимог закону щодо збору, обробки та використання даних. Це означає, що недозволені дії, такі як незаконне збирання чи передача даних, порушують цей принцип.

Принцип законності захисту персональних даних спрямований на забезпечення прав та свобод громадян в сфері обробки їхніх персональних даних та запобігання можливим зловживанням з боку організацій чи осіб, які мають доступ до цих даних.

Регламент Європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Далі – Регламент ЄС) був прийнятий задля розширення дії Директиви 95/46/ЄС, яка втратила свою чинність. Регламентом ЄС визначено, що принципи і норми щодо захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних передбачають, незалежно від їхнього громадянства або місця проживання, дотримання їхніх фундаментальних прав і свобод, зокрема їхнього права на захист персональних даних. Регламент ЄС спрямовано на сприяння формуванню простору свободи, безпеки і правосуддя, економічного союзу, соціально-економічному прогресові, зміцненню та конвергенції економік у межах внутрішнього ринку, підтриманню добробуту фізичних осіб.

Принципи захисту даних необхідно застосовувати до будь-якої інформації про фізичну особу, яку ідентифіковано чи можна ідентифікувати. Персональні дані із використанням псевдоніму, що можна приписати фізичній особі після використання додаткової інформації, необхідно розглядати як інформацію про фізичну особу, яку можна ідентифікувати. Принципи захисту даних, відповідно, не можна застосовувати до анонімної інформації, зокрема інформації, що не стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати, або персональних даних, що стали анонімними у такий спосіб, що суб'єкта даних неможливо чи більше неможливо ідентифікувати. Таким чином цей Регламент не стосується опрацювання такої анонімної інформації, у тому числі, для статистичних або дослідницьких цілей.

Можна зауважити, що Регламент ЄС, дає чітке визначення інформації, яку можна віднести до персональних даних. Також визначено про такий вид інформації, як анонімна інформація. Закон України «Про захист персональних даних», має більш вужчий характер, ніж Регламент ЄС та є деякі аспекти не врегульовані цим Законом.

Будь-яке опрацювання персональних даних повинно бути законним та правомірним. Фізичні особи повинні бути обізнані про те, що їхні персональні дані збирають, використовують, обговорюють або іншим чином опрацьовують, а також про те, якою мірою опрацьовують чи опра-

цьовуватимуть персональні дані. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо опрацювання таких персональних даних були доступними і зрозумілими, з використанням чітких і простих формулювань. Цей принцип стосується, зокрема, інформування суб'єктів даних про особу контролера та цілі опрацювання і надання подальшої інформації для забезпечення правомірного і прозорого опрацювання в частині, що стосується відповідних фізичних осіб та їхнього права на отримання підтвердження та повідомлення про ті персональні дані, які їх стосуються та підлягають опрацюванню. Фізичні особи повинні бути обізнані про ризики, правила, гарантії та права щодо опрацювання персональних даних і про те, як реалізувати свої права у зв'язку з таким опрацюванням. Зокрема, спеціальні цілі опрацювання персональних даних повинні бути прямо вираженими та законними, а також означеними на момент збирання персональних даних.[1]

Принцип відкритості та прозорості використання персональних даних означає, що обробка персональних даних здійснюється відкрито для самого суб'єкта даних, тобто, особа має право у будь-який час звернутися до держателя персональних даних для отримання актуальної інформації про себе.

Крім того, особа, яка надає свої персональні дані, має право знати для якої мети обробляються її персональні дані, які треті особи мають до них доступ тощо, Суб'єкт даних повинен мати право доступу до персональних даних, які збирають щодо нього, та реалізовувати таке право вільно та в розумні строки для того, щоб бути обізнаним про законність опрацювання та перевірки такої інформації.

Принцип прозорості вимагає, щоб будь-яка інформація, призначена для громадськості або суб'єкта даних, була стислою та зрозумілою, з використанням чітких та простих формулювань, а також, за необхідності, із застосуванням засобів візуалізації. Таку інформацію можна надавати в електронному форматі, наприклад, через веб-сайт. Це, зокрема, є доцільним у ситуаціях, коли збільшення кількості агентів та технологічна складність практичної діяльності перешкоджають обізнаності та розумінню суб'єкта даних того, чи збирають її або його персональні дані, хто їх збирає та для якої цілі, як, наприклад, у випадку онлайн-реклами [1].

Принцип прозорості захисту персональних даних є ключовим аспектом у сфері правового регулювання обробки та використання персональної інформації громадян в Україні. Цей принцип передбачає, що суб'єкти персональних даних мають чітку та доступну інформацію про те, як їхні дані збираються, обробляються та використовуються, а також про свої права та обов'язки у цьому контексті.

Відповідно до Закону України «Про захист персональних даних», організації та суб'єкти персональних даних повинні надавати інформацію про цілі обробки даних, отримувачів даних, строк зберігання, права суб'єкта персональних даних тощо. Прозорість також вимагає вказати, яким чином можна відкликати згоду на обробку даних, якщо вона була надана, та як звертатися до організації з питань захисту персональних даних.

Щоб забезпечити прозорість захисту персональних даних, організації мають розробляти політики конфіденційності, які повинні бути доступні для ознайомлення для всіх зацікавлених осіб. Також, вони зобов'язані інформувати суб'єктів персональних даних про будь-які зміни в політиці конфіденційності та використовувати зрозумілу та доступну мову.

Додатковою вимогою є надання можливості суб'єкту персональних даних контролювати свої дані та забезпечувати їхню точність. Це може включати можливість виправляти неправильні дані або вимагати видалення інформації.

Для того щоб відстоювати свої права, згідно із Законом України «Про захист персональних даних» [5], суб'єкт персональних даних повинен мати чітке уявлення про:

– мету збору персональних даних (має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних);

– володільця персональних даних (фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом);

– розпорядника персональних даних (фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця);

– склад та зміст персональних даних (мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки).

Окремо суб'єкта персональних даних зобов'язаний бути обізнаним в своїх правах. Так, статтею 8 Закону [5] передбачено такі права суб'єкта персональних даних:

– знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних;

– отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

– на доступ до своїх персональних даних;

– отримувати не пізніше, як за тридцять календарних днів із дня надходження запиту (крім випадків, передбачених законом), відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

– пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

– пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

– на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

– звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

– застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

– вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

– відкликати згоду на обробку персональних даних;

– знати механізм автоматичної обробки персональних даних;

– на захист від автоматизованого рішення, яке має для нього правові наслідки.

Безпека особистих даних залежить не тільки від норм, встановлених нормативно-правовими актами, а й враховування всіх ризиків, та здійснення всіх заходів, задля уникнення витоку інформації. Саме таку мету також переслідує Регламент ЄС

Варто відзначити, що у ЄС норми Регламенту мають пряму дію та обов'язкові до застосування усіма державами-членами.

Так, новим документом, зокрема, передбачається:

– демонстрація (доведення) відповідності вимогам GDPR;

– підвищення рівня безпеки персональних даних;

– запровадження контролю за передачею персональних даних за межі Європейського економічного простору;

– обмеження можливості використання хмарних сховищ для розміщення персональних даних;

– загальне підвищення рівня приватності;

– вдосконалена процедура повідомлення про витік даних;

– зміцнення контролю у відносинах між контролерами та обробниками;

– обмеження можливості залучення субобробників;

Переходячи до згоди на обробку персональних даних, то знову звернемося до Регламенту ЄС, де вказано, що згоду необхідно надавати шляхом чіткого ствердження, що становить вільно надане, конкретне, проінформоване та однозначне свідчення погодження суб'єкта даних на опрацювання його або її персональних даних, зокрема, у формі письмової заяви, в тому числі електронними засобами, або у формі усної заяви. Це може включати заповнення клітинки позначкою під час відвідування веб-сайту в мережі Інтернет, обрання технічних налаштувань для послуг інформаційного суспільства або іншу заяву чи поведінку, що чітко вказують на погодження суб'єктом даних із запропонованим опрацюванням персональних даних. Мовчання, автоматичне заповнення клітинок позначками або бездіяльність, відповідно, не становлять надання згоди. Згода повинна поширюватися на всі види опрацювання даних, що здійснюють для однакової цілі або цілей. У разі, якщо опрацювання передбачає досягнення множинних цілей, згода потрібна для кожної з них. Якщо згоду суб'єкта даних необхідно надати після електронного запиту, у такому разі запит

повинен бути чітким, точним та не мати надмірно негативних наслідків для використання послуги, для якої його надають.

Часто на момент збирання даних неможливо повністю визначити мету опрацювання персональних даних для цілей наукового дослідження. Тому, суб'єкти даних повинні мати дозвіл на надання згоди на деякі сфери наукових досліджень, якщо в них дотримано визнаних етичних норм для наукового дослідження. Суб'єкти даних повинні мати можливість надавати свою згоду лише на окремі сфери дослідження або частини дослідницьких проектів в обсязі, виправданому поставленою метою.

Висновки. У цій статті були проаналізовані два ключові принципи захисту персональних даних в Україні - прозорість та згода. Вивчення цих принципів свідчить про їхню важливість та актуальність у сучасному цифровому суспільстві.

Принцип прозорості визначає необхідність доступної та зрозумілої інформації для суб'єктів персональних даних щодо процесів обробки їхніх даних. Відкритість є фундаментальною вимогою для підтримання довіри між організаціями та громадянами. Забезпечення можливості контролю та регулювання своїх даних дозволяє суб'єктам даних більш активно брати участь у процесах обробки та використання їхніх персональних даних.

Принцип згоди, у свою чергу, робить акцент на добровільний та інформований характер дозволу на обробку даних. Згода суб'єкта даних визначає підставу для легальної обробки персональних даних, забезпечуючи гармонію між правами громадян та інтересами організацій. Завдяки цьому принципу суб'єкти даних можуть визначати, які дані вони надають та як вони можуть бути використані, що важливо для збереження їхньої конфіденційності та контролю над власною інформацією.

Враховуючи розвиток технологій та зміни в законодавстві, прозорість та згода виявляються ще більш важливими аспектами. Вони допомагають підтримувати баланс між правами суб'єктів даних та необхідністю організацій у здійсненні обробки даних для досягнення своїх цілей.

Наслідки неправильної інтерпретації або невідповідності цих принципів можуть включати порушення конфіденційності, недовіру споживачів та юридичні наслідки для організацій, які здійснюють збір, обробку та захист персональних даних. Тому, впровадження та дотримання прозорості та згоди є необхідним завданням для всіх суб'єктів, що займаються обробкою персональних даних в Україні.

У цілому, забезпечення прозорості та відповідності принципам згоди є важливою передумовою для підвищення довіри громадян до цифрових сервісів та забезпечення належного захисту їхніх персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Регламент Європейського парламенту І Ради (ЄС) 2016/679 від 27 квітня 2016 року URL: https://zakon.rada.gov.ua/ laws/show/984_008-16#Text.
2. Колодій В.М. Принципи права: генеза, поняття, класифікація та реалізація. *Альманах права*. 2012. Вип. 3. С. 42–46.
3. Волошин Ю.О. Принцип. Юридична енциклопедія: В 6 т. / [за ред. Ю.С. Шемшученко (голова ред. кол.) та ін.]. К. Вид-во «Українська енциклопедія» імені М.П. Бажана. 1998–2004. Т. 5. 2003. С. 110-111.
4. Зайчук О.В. Принципи права в контексті розвитку загальної теорії держави і права. URL: http://dspace.nbuv.gov.ua/bitstream/handle/ 123456789/63854/04-Zaychuk.pdf?sequence=1.
5. Про захист персональних даних. Закон України від 01 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
6. Бєлова М.В., Бєлов Д.М., Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник УжНУ. Серія «Право».* Випуск 79(5). 2023. С. 289–294.
7. Бєлов Д.М., Бєлова М.В., Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник УжНУ. Серія «Право».* Випуск 78(4). Ч. 3. 2023. С. 122–129.