
Варшава, 13 червня 2025 року
Висновок №: TERR-UKR/526/2025 [NR]

ВИСНОВОК ЩОДО ПРОЄКТУ ЗАКОНУ УКРАЇНИ «ПРО ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПРО ПАСАЖИРІВ ДЛЯ ПРОТИДІЇ ТЕРОРИЗМУ, ТЯЖКИМ ТА ОСОБЛИВО ТЯЖКИМ ЗЛОЧИНАМ»

УКРАЇНА

У підготовці цього Висновку були використані матеріали, надані **паном Карімом Лабібом**, старшим експертом з кримінального права, протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) та протидії тероризму; та **пані Назлі Ілдірим Шерколк**, незалежною експерткою з питань реформування сектору безпеки та прав людини.

На основі наданого Службою безпеки України неофіційного перекладу проекту Закону англійською мовою.



Бюро з демократичних інститутів і прав людини ОБСЄ

Ul. Miodowa 10, PL-00-251 Warsaw
Офіс: +48 22 520 06 00, Факс: +48 22 520 0605
www.legislationline.org

РЕЗЮМЕ Й ОСНОВНІ РЕКОМЕНДАЦІЇ

Розробка проекту Закону «Про використання інформації про пасажирів для протидії тероризму, тяжким та особливо тяжким злочинам» знаменує собою значні та своєчасні зусилля України, спрямовані на створення всеосяжної правової бази для обробки попередньої інформації про пасажирів (API) та даних запису реєстрації пасажирів (PNR) в контексті повітряних перевезень. Багато положень проекту Закону відповідають міжнародним зобов'язанням, проте залишаються прогалини, які перешкоджають повному дотриманню міжнародних стандартів захисту персональних даних і права на недоторканність приватного життя, що впливають з міжнародних і регіональних документів у сфері прав людини. Проект Закону можна також удосконалити для недопущення надмірного впливу на право осіб на свободу пересування, а також прямого чи опосередкованого порушення права осіб, які потребують особливого захисту, як-от біженці та шукачі притулку, діти та жертви торгівлі людьми. Так, слід внести деякі корективи, зокрема, щодо обмеження мети обробки персональних даних, пропорційності, зберігання даних, автоматизованої обробки, передачі даних та індивідуальних прав.

Уточнення сфери застосування проекту Закону з метою чітко обмежити обробку даних чітко визначеними терористичними та тяжкими злочинами, що мають прямий чи опосередкований зв'язок з авіаперевезеннями, допоможе забезпечити дотримання принципу обмеження мети та запобігти надмірно широкому застосуванню. Аналогічно, скорочення терміну зберігання даних PNR до шести місяців, з можливістю продовження до п'яти років лише за наявності об'єктивної та конкретної потреби, краще відповідатиме вимогам пропорційності.

Запровадження надійних гарантій для автоматизованої обробки даних, включаючи обов'язкову перевірку людиною, виключення дискримінаційного профілювання та чіткі, об'єктивні критерії, посилить захист від потенційного свавільного застосування. Було б також корисно укріпити права фізичних осіб шляхом внесення чіткої норми про надання їм доступу до їхніх даних, можливості їх виправлення або видалення, а також про ефективні засоби правового захисту у випадку неправомірного використання.

Упровадження рекомендованих змін сприятиме дотриманню вимог міжнародних і регіональних документів у сфері прав людини та забезпечить кращий баланс між цілями безпеки та зобов'язаннями щодо дотримання прав людини.

На додаток до викладеного вище, БДІПЛ надає такі рекомендації для забезпечення більшої відповідності проекту Закону чинним регіональним і міжнародним стандартам у сфері прав людини та зобов'язанням у рамках ОБСЄ:

А. Щодо обмеження мети:

1. узгодити з міжнародними стандартами мету збору даних PNR, а саме з метою запобігання, виявлення, розслідування та кримінального переслідування виключно терористичних злочинів та тяжких злочинів, щоби не допустити непропорційного збирання даних та їх використання як інструменту масового спостереження, що виходить за межі цілей, визначених міжнародними стандартами; [параграф 58]
 2. включити до проекту Закону положення про негайне та безповоротне видалення Національним контактним пунктом інших персональних даних третіх осіб після їх отримання; [параграф 60]
- В. забезпечити, щоби збір даних обмежувався лише тими даними, які є строго необхідними для запобігання, виявлення, розслідування та переслідування тероризму та тяжких злочинів відповідно до принципу мінімізації даних, а також передбачити чітке положення про обов'язок негайного та безповоротного видалення даних, які виходять за межі встановлених у проекті Закону категорій, у тому числі будь-яких чутливих даних; [параграф 63]
- С. відобразити у статті 18 проекту Закону, що
- неавтоматизована перевірка повинна виключати будь-які дискримінаційні результати;
 - Національний контактний пункт не передає компетентним органам результати автоматизованої обробки, якщо за результатами такої перевірки він дійде висновку про відсутність підстав, які могли б відповідно до застосовних правових стандартів викликати обґрунтовану підозру в причетності до терористичних злочинів або тяжких злочинів осіб, ідентифікованих за допомогою автоматизованої обробки, або якщо він має підстави вважати, що така обробка призведе до дискримінаційного результату;
 - Національний контактний пункт встановлює в чіткий і точний спосіб об'єктивні критерії перевірки, що дозволяють співробітникам Національного контактного пункту, відповідальним за індивідуальну перевірку, з одного боку, з'ясувати, чи стосується і якщо так, то якою мірою, позитивний збіг тієї особи, яка може бути причетною до терористичних злочинів або тяжких злочинів, а тому має пройти додаткову перевірку з боку компетентних органів, як передбачено Статтею 7 Директиви ЄС про PNR, а з іншого боку, пересвідчитись у недискримінаційному характері автоматизованої обробки даних і, зокрема, заздалегідь встановлених критеріїв і використовуваних баз даних;
 - Будь-які заздалегідь встановлені критерії, за якими порівнюються дані PNR, не призводять до незаконної диференціації та забезпечують виключення дискримінаційних результатів;
 - До цього положення включено захисне застереження щодо заяв про надання притулку; [параграфи 68-70]
- Д. чітко визначити перелік уповноважених органів у самому проекті Закону або в додатку до нього, або зробити посилання на відповідне законодавство, яке регулює діяльність цих уповноважених органів, а

також розробити механізми незалежної перевірки перед наданням відповіді на належно обґрунтований запит компетентних органів з метою запобігання, виявлення, розслідування та переслідування терористичних злочинів або тяжких злочинів; [параграфи 71-72]

- Е. передбачити у Статті 24 проєкту Закону, що перед укладанням угоди про обмін даними API/PNR або перед обміном такими даними на *разовій* основі слід провести оцінку стану дотримання прав людини та захисту даних іншою стороною, а також оцінку правових гарантій та інституційного контролю, які регулюють діяльність органу-одержувача, щоби переконатися, що третя країна дотримується еквівалентних стандартів захисту. Така угода також повинна переглядатися з певною регулярністю або за необхідності; [параграф 82]
- Ф. запровадити ефективні гарантії дотримання прав людини для захисту пасажирів від неправомірної підозри у причетності до тероризму або інших тяжких злочинів та утриматися від дискримінаційного профілювання на основі даних PNR у переліку завдань Національного контактного пункту, наведеному в статті 15. Критерії ризику та профілі повинні бути цільовими, пропорційними та конкретними, а також зобов'язувати відповідні органи надавати необхідні настанови для проведення індивідуальних перевірок з метою запобігання дискримінаційним результатам; [параграф 86]
- Г. роз'яснити у статті 21 проєкту Закону, що співробітники з питань захисту даних PNR можуть безпосередньо та конфіденційно повідомляти про порушення Уповноваженому Верховної Ради України з прав людини, а також можуть передавати справи на розгляд Уповноваженого та вживати інших заходів; [параграф 95] та
- Н. забезпечити, щоби будь-який нагляд за дотриманням законодавства про захист даних незалежно здійснювався уповноваженим органом, якому надано необхідні ресурси та повноваження для виконання свого мандату у спосіб, що відповідає міжнародним документам, а також забезпечити, щоби цей орган або Уповноважений Верховної Ради України з прав людини мав повний і безперешкодний доступ до всієї інформації, що обробляється Національним контактним пунктом, а також до заздалегідь визначених критеріїв і баз даних, необхідних для виконання свого мандату. [параграфи 98-99].

До тексту Висновку входять вищенаведені та додаткові рекомендації, виділені жирним шрифтом.

У межах свого мандату з надання допомоги державам-учасницям ОБСЄ щодо виконання їхніх зобов'язань в рамках ОБСЄ у сфері людського виміру, БДІПЛ за запитом розглядає законопроєкти та чинні закони з метою оцінити їх відповідність міжнародним

Висновок щодо проекту Закону України «Про використання інформації про пасажирів для протидії тероризму, тяжким та особливо тяжким злочинам»

стандартам прав людини та зобов'язанням в рамках ОБСЄ, а також надає конкретні рекомендації щодо їх удосконалення.

ЗМІСТ

I. ВСТУП.....	7
II. ОБСЯГ АНАЛІЗУ	7
III. ПРАВОВИЙ АНАЛІЗ І РЕКОМЕНДАЦІЇ	8
1. Відповідні міжнародні стандарти прав людини та зобов'язання ОБСЄ у сфері людського виміру	8
1.1. Стандарти щодо збору, обробки й обміну даними в контексті авіап перевезень	9
1.2. Захист даних і право на повагу до приватного життя.....	15
1.2.1 Право на повагу до приватного життя	16
1.2.2 Право на захист даних	18
1.2.3 Потенційний вплив на інші права людини й основоположні свободи	22
2. Передумови	24
3. Збір, обробка та обмін даними API/PNR	24
3.1. Обмеження мети	24
3.2. Збір та обробка даних API/PNR.....	27
3.3. Автоматизована обробка	28
3.4. Обмін даними з уповноваженими органами	31
3.5. Зберігання даних	33
3.6. Міжнародне співробітництво	34
4. Недискримінація.....	36
5. Обов'язок інформувати та безпека персональних даних	38
6. Незалежний нагляд	41
7. Механізми оскарження та судового контролю	42
8. Рекомендації щодо процесу підготовки й ухвалення проєкту Закону	43

ДОДАТОК: Проєкт Закону України «Про використання інформації про пасажирів для протидії тероризму, тяжким та особливо тяжким злочинам»

I. ВСТУП

1. 20 вересня 2024 року заступник Голови Служби безпеки України звернувся до Бюро з демократичних інститутів і прав людини ОБСЄ (далі – БДПІЛ) із запитом про здійснення правової експертизи проєкту Закону України «Про використання інформації про пасажирів для протидії тероризму, тяжким та особливо тяжким злочинам» (далі – проєкт Закону).
2. 17 жовтня 2024 року БДПІЛ відповіло на цей запит, підтвердивши готовність Бюро підготувати правовий висновок щодо відповідності проєкту Закону міжнародним стандартам прав людини та зобов'язанням ОБСЄ у сфері людського виміру. З огляду на предмет дослідження, БДПІЛ запросило Відділ з питань безпеки й управління кордонами Секретаріату ОБСЄ зробити свій внесок у підготовку цього юридичного висновку.
3. Цей Висновок підготовлено у відповідь на вищезазначений запит. БДПІЛ здійснило правову оцінку в межах свого мандату з надання допомоги державам-учасникам ОБСЄ у виконанні їхніх зобов'язань у сфері людського виміру ОБСЄ.¹

II. ОБСЯГ АНАЛІЗУ

4. Цей Висновок охоплює лише проєкт Закону, наданий для аналізу. Відтак, зважаючи на обмежений об'єкт аналізу, Висновок не є повним і всебічним оглядом усієї правової та інституційної бази, що регулює збір інформації з метою протидії тероризму, тяжким та особливо тяжким злочинам в Україні.
5. У Висновку порушено ключові питання та зазначено сфери, що викликають занепокоєння. З міркувань лаконічності, основну увагу в ньому приділено положенням, що потребують перегляду чи вдосконалення, радше ніж позитивним аспектам проєкту Закону. Подальший правовий аналіз ґрунтується на міжнародних і регіональних стандартах, нормах і рекомендаціях у сфері прав людини та верховенства права, а також на відповідних зобов'язаннях ОБСЄ у сфері людського виміру. У Висновку також висвітлюється, коли це доречно, передовий досвід інших держав-учасниць ОБСЄ у цій сфері. Посилаючись на національне законодавство, БДПІЛ не пропагує якусь конкретну модель країни; воно радше прагне надати чітку інформацію про застосовні міжнародні стандарти, ілюструючи при цьому, як вони реалізуються на практиці у певних національних законах. До прикладу будь-якої країни завжди слід підходити з обережністю, оскільки він не обов'язково може бути відтворений в іншій країні й має розглядатися у світлі ширшої національної інституційної та правової системи, а також контексту та політичної культури країни.
6. Крім того, відповідно до *Конвенції про ліквідацію всіх форм дискримінації щодо жінок*² (далі – КЛДЖ) та *Плану дій ОБСЄ 2004 року з підтримки гендерної рівності*,³ а також зобов'язань щодо інтеграції гендерної проблематики в

1 Зокрема, БДПІЛ провело цю оцінку в межах свого мандату, визначеного Бухарестським планом дій ОБСЄ з боротьби з тероризмом. Див. пункти 6, 18 і 22 Додатку до Рішення Ради міністрів ОБСЄ MC(9).DEC/1, Бухарест, 3-4 грудня 2001 року.

2 Конвенція ООН про ліквідацію всіх форм дискримінації щодо жінок (далі – КЛДЖ), ухвалена Генеральною Асамблеєю ООН, резолюція 34/180 від 18 грудня 1979 року. Україна здала на зберігання свою ратифікаційну грамоту 12 березня 1981 року.

3 План дій ОБСЄ з підтримки гендерної рівності, ухвалений Рішенням № 14/04, MC.DEC/14/04 (2004), п. 32.

діяльність, програми та проекти ОБСЄ, цей Висновок включає, де це доцільно, гендерну перспективу та перспективу різноманіття.

7. Висновок підготовлено на основі неофіційного перекладу проекту Закону англійською мовою, наданому Службою безпеки України, що міститься у Додатку до цього документу. Тому можливі неточності, пов'язані з перекладом. Висновок також доступний українською мовою. Однак версія англійською мовою залишається єдиною офіційною версією Висновку.
8. З огляду на вищевикладене, БДПЛ хотіло би підкреслити, що цей Висновок жодним чином не утримує БДПЛ від будь-яких додаткових письмових або усних рекомендацій чи коментарів з відповідних питань в Україні, що їх Бюро може зробити в майбутньому.

III. ПРАВОВИЙ АНАЛІЗ І РЕКОМЕНДАЦІЇ

1. ВІДПОВІДНІ МІЖНАРОДНІ СТАНДАРТИ ПРАВ ЛЮДИНИ ТА ЗОБОВ'ЯЗАННЯ ОБСЄ У СФЕРІ ЛЮДСЬКОГО ВИМІРУ

9. Упродовж останніх десятиліть зростає кількість людей, що подорожують повітряним транспортом. Водночас інновації, що призвели до збільшення розмірів літаків, зумовили потребу в більш ефективному та раціональному обслуговуванні пасажиропотоків в аеропортах. У 2019 році Міжнародна організація цивільної авіації (далі – ІКАО) повідомила, що на регулярних рейсах повітряного транспорту по всьому світі було перевезено 4,5 мільярда пасажирів.⁴ Ці пасажиропотоки чинять дедалі більший тиск на міжнародні повітряні кордони. На цьому тлі за останнє десятиліття зросла кількість міжнародних і регіональних юридично зобов'язальних документів і інструментів м'якого права щодо збору, обробки й обміну попередньою інформацією про пасажирів (API) і даними запису реєстрації пасажирів (PNR), особливо в контексті боротьби з тероризмом та іншими тяжкими злочинами.
10. Дані API – це комплекс інформації про подорожніх, безпосередньо взятої з їхніх паспортів, у поєднанні з інформацією про рейс, зібраною під час реєстрації на рейс і переданою прикордонним органам країни призначення. Обробка API є інструментом управління кордонами, спрямованим на підвищення ефективності та результативності прикордонних перевірок шляхом спрощення та прискорення оформлення подорожніх, а також інструментом протидії нелегальній імміграції.⁵
11. Дані PNR – це неперевірена інформація, яку пасажир надає безпосередньо або через туристичні агенції, а авіаперевізники збирають для забезпечення процесів бронювання та реєстрації. Аналіз даних PNR може надати компетентним органам важливі елементи кримінальної розвідки, дозволяючи виявляти підозрілі схеми подорожей та ідентифікувати спільників злочинців і терористів, зокрема тих, які раніше не були відомі правоохоронним органам.⁶

⁴ Міжнародна організація цивільної авіації (ІКАО), [Світ повітряного транспорту в 2019 році](#).

⁵ [SOM \(2022\) 729 Пропозиція щодо Регламенту Європейського Парламенту та Ради про збір та передачу попередньої інформації про пасажирів \(API\) для посилення та полегшення зовнішнього прикордонного контролю](#), що вносить зміни до Регламенту (ЄС) 2019/817 та Регламенту (ЄС) 2018/1726 та скасовує Директиву Ради 2004/82/ЄС (далі – Пропозиція ЄС щодо API), с. 1,

⁶ [Європейська Комісія - Дані про пасажирів](#).

12. Збір персональних даних, що містяться в наборах даних API та PNR, їх використання, обмін та обробка, які також можуть впливати на ухвалення рішень на міжнародних кордонах, мають серйозні наслідки для прав осіб на повагу до приватного та сімейного життя, свободу пересування (права осіб залишати будь-яку країну і повертатись у країну походження) та шукати притулку, а також, можливо, інших основних прав і свобод (зокрема, свободи вираження поглядів, участі в політичному житті, свободи мирних зібрань, свободи об'єднання, свободи релігії та переконань), а також права на свободу від дискримінації.
13. Слід одразу підкреслити, що необхідність і пропорційність нецільового, масового збору й обробки даних про пасажирів з метою протидії тероризму та іншим тяжким злочинам були поставлені під сумнів – зокрема, через відсутність серйозних, надійних і перевірених доказів, що підтверджують їхню дієвість, а також через побоювання щодо надійності таких систем, особливо з огляду на те, що навіть невеликі помилки можуть мати значні наслідки, коли вони стосуються дуже великої кількості авіапасажирів.⁷ Оцінка необхідності й ефективності таких схем виходить за рамки цього Висновку, проте цей правовий аналіз має на меті надати рекомендації задля забезпечення відповідності схеми API/PNR, передбаченої проєктом Закону, міжнародним стандартам у сфері прав людини та зобов'язанням в рамках ОБСЄ.

1.1. Стандарти щодо збору, обробки й обміну даними в контексті авіаперевезень

14. У системі ООН, у контексті боротьби з тероризмом, Рада Безпеки Організації Об'єднаних Націй (далі – РБ ООН) ухвалила кілька резолюцій, що закликають держави-члени й авіакомпанії збирати й обробляти відповідні дані про пасажирів. У 2014 році Резолюція РБ ООН 2178 закликала держави-члени ООН вимагати від авіакомпаній, що здійснюють діяльність на їхній території, завчасно надавати API відповідним національним органам влади з метою виявлення виїзду з їхньої території або спроб в'їзду на їхню територію чи транзиту через неї цивільними повітряними суднами осіб, визначених Комітетом, заснованим резолюціями 1267 (1999) і 1989 (2011) (і пізніше 2253 (2015)) (Комітет РБ ООН). Крім того, Резолюція закликала держави-члени ООН повідомляти Комітету РБ ООН про будь-який такий виїзд з їхньої території, або такі спроби в'їзду на їхню територію або транзиту через неї таких осіб, а також направляти цю інформацію державі проживання або громадянства, в залежності від обставин та відповідно до внутрішнього законодавства і міжнародних зобов'язань.⁸
15. Ухвалена у 2016 році Резолюція РБ ООН 2309 вимагала, щоб «авіакомпанії, які здійснюють свою діяльність на їхній території, заздалегідь надавали інформацію про пасажирів відповідним національним органам влади для виявлення виїзду з їхньої території або спроб в'їзду на їхню територію чи транзиту через неї цивільними повітряними суднами осіб, визначених Комітетом відповідно до резолюцій 1267 (1999), 1989 (2011) і 2253 (2015)».⁹

⁷ Див., наприклад, Висновки Європейського інспектора із захисту даних, особливо Висновок [5/2015 щодо Директиви ЄС про PNR](#) та [Висновок щодо проєкту угоди між ЄС та Канадою](#); див. також Спеціальний доповідач з питань просування та захисту прав людини й основних свобод в умовах боротьби з тероризмом, [Позиційний документ щодо Програми Організації Об'єднаних Націй з протидії подорожам, пов'язаним з тероризмом \(CT Travel\), та програмне рішення goTravel](#) (2023). Див. також БДПІЛ, [Аналітична записка: Управління кордонами та права людини – Збір, обробка й обмін персональними даними та використання нових технологій у контексті боротьби з тероризмом і забезпечення свободи пересування](#) (2021), с. 13, та посилання в цьому документі.

⁸ Комітет РБ ООН відповідно до резолюцій 1267 (1999), 1989 (2011) і 2253 (2015) щодо Ісламської держави Іраку й Ліванту (ІДІЛ), Аль-Каїди та пов'язаних з ними осіб, груп, підприємств і організацій; див. РБ ООН, [S/RES/2178 \(2014\)](#), п. 9

⁹ РБ ООН, [S/RES/2309 \(2016\)](#), п. 6g.

16. У грудні 2017 року Рада Безпеки ООН одногосно ухвалила Резолюцію 2396.¹⁰ Спираючись на попередні резолюції 2178 (2014) та 2309 (2016), вона встановила, що держави-члени ООН повинні збирати дані API та PNR. Оскільки Резолюція РБ ООН 2396 була ухвалена відповідно до Глави VII Статуту ООН і містить формулювання, що вказують на намір надати їй зобов'язальну силу,¹¹ дотримання цього зобов'язання є обов'язковим для всіх держав-членів ООН. Резолюція встановлює, що держави «...зобов'язані вимагати від авіакомпаній, що здійснюють діяльність на їх території, надавати API відповідним національним органам згідно з внутрішнім законодавством і міжнародними зобов'язаннями...» та «...забезпечити аналіз API всіма компетентними органами, з повною повагою до прав людини й основних свобод з метою запобігання, виявлення та розслідування терористичних злочинів та перевезень, пов'язаних з терористичною діяльністю...».¹² Резолюція також постановляє, що «...держави-члени повинні розвивати потенціал для збору, обробки й аналізу, відповідно до стандартів і рекомендованої практики ІКАО, даних записів реєстрації пасажирів (PNR) і забезпечити використання даних PNR і обмін ними з усіма своїми компетентними національними органами з повною повагою до прав людини і основних свобод з метою запобігання, виявлення і розслідування терористичних злочинів ... а також закликає ІКАО працювати зі своїми державами-членами над встановленням стандарту для збору, використання, обробки і захисту даних PNR».¹³
17. Іншим ключовим інструментом у цій сфері є Конвенція про міжнародну цивільну авіацію (також відома як Чиказька конвенція).¹⁴ Стаття 37 Чиказької конвенції зобов'язує Міжнародну організацію цивільної авіації (ІКАО) «приймати і в міру необхідності час від часу змінювати міжнародні стандарти, рекомендовану практику і процедури, що стосуються митних та імміграційних процедур...».¹⁵ У цьому контексті ІКАО розробила «Міжнародні стандарти та рекомендовану практику», які є Додатком 9 до Чиказької конвенції. Стандарти та практики регулярно оновлюються, востаннє – у липні 2022 року.¹⁶ Глава 9 Додатку 9 присвячена виключно системам обміну даними про пасажирів, в якій викладено стандарти та практики регулювання API та PNR. Додаток 9 встановлює надійні стандарти та гарантії щодо аспектів захисту персональних даних при регулюванні API/PNR, зокрема щодо гарантій законності, необхідності та пропорційності, стандартів доступу до PNR і обов'язку інформувати суб'єкта даних, запобіжників проти автоматизованої обробки даних PNR, стандартів незалежного нагляду за даними PNR, запобіжників проти дискримінації, а також стандартів і рекомендованої практики обробки даних PNR.¹⁷
18. У грудні 2016 року Рада міністрів ОБСЄ ухвалила Рішення № 6/16 «Посилення використання попередньої інформації про пасажирів», яке зобов'язує держави-учасниці створити національні системи API відповідно до положень, що містяться

10 РБ ООН, [S/RES/2396 \(2017\)](#).

11 Хоча РБ ООН має загальні повноваження відповідно до статей 24 і 25 Статуту ООН ухвалювати обов'язкові до виконання рішення, які не завжди повинні ухвалюватися відповідно до Глави VII Статуту ООН, обов'язковість положень резолюції РБ ООН повинна визначатися в кожному конкретному випадку з урахуванням умов резолюції, що підлягають тлумаченню, обговорення, що призвело до її ухвалення, положень Статуту, на які вони посилаються, і, загалом, всіх обставин, які можуть допомогти у визначенні правових наслідків резолюції Ради Безпеки. Міжнародний суд ООН, [Консультативний висновок щодо юридичних наслідків для держав триваючої присутності Південної Африки в Намібії \(Південно-Західна Африка\), незважаючи на резолюцію 276 \(1970\) Ради Безпеки](#), 21 червня 1971 року, пп. 113-114.

12 РБ ООН, [S/RES/2396 \(2017\)](#), п. 11.

13 РБ ООН, [S/RES/2396 \(2017\)](#), п. 12.

14 Україна подала повідомлення про приєднання 10 серпня 1992 року.

15 [Конвенція про міжнародну цивільну авіацію](#) (Чиказька конвенція) була підписана 7 грудня 1944 року 52 державами. Україна подала документ про приєднання до Чиказької конвенції 10 серпня 1992 року.

16 ІКАО, [Додаток 9 до Конвенції про міжнародну цивільну авіацію, Міжнародні стандарти та рекомендована практика](#), Шістнадцяте видання, липень 2022 року.

17 Чиказька конвенція, Додаток 9, [Глава 9](#).

в Додатку 9 до Чиказької конвенції ІКАО та узгоджені з Керівними принципами ІКАО щодо АРІ, в тому числі щодо конфіденційності та захисту даних, з метою ефективного збору даних про пасажирів та/або членів екіпажів від авіакомпаній, що здійснюють діяльність на їхній території.¹⁸ Варто зазначити, що Рішення ОБСЄ містить пряме посилення на стандарти конфіденційності та захисту даних.

19. На рівні Ради Європи у зв'язку з цією темою слід також брати до уваги [Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних](#)¹⁹ та [Конвенцію про доступ до офіційних документів](#)²⁰.
20. Як кандидат на вступ до Європейського Союзу, Україна також повинна привести своє національне законодавство у відповідність до законодавства ЄС, а отже, відповідні положення договорів, регламентів і директив ЄС є також актуальними для цього Висновку. У зв'язку з цим слід зазначити, що проект Закону розроблено в рамках комплексної оцінки транспозиції правових стандартів Європейського Союзу в законодавство України та з метою імплементації Директиви ЄС про PNR, спрямованої на законодавче регулювання отримання, обробки й використання такої інформації для протидії тероризму та тяжким злочинам.
21. В Європейському Союзі (ЄС) збір, обробка та обмін даними АРІ/PNR регулюється Директивами, що є обов'язковими для виконання державами-членами ЄС щодо результатів, які мають бути досягнуті, та повинні бути імplementовані в національне законодавство. 27 квітня 2016 року Європейський Парламент і Рада ухвалили Директиву про використання даних PNR для запобігання, виявлення, розслідування та переслідування терористичних злочинів і тяжких злочинів (далі – Директива ЄС про PNR).²¹ Директива визначає обов'язки держав-членів ЄС щодо збору даних PNR, вимагаючи від них створення спеціальних органів, відповідальних за збір, зберігання й обробку даних PNR (так звані підрозділи з питань інформації про пасажирів (PIU)), а також затвердження переліку компетентних органів, які мають право запитувати чи отримувати дані PNR. Зазначені підрозділи відповідають за збір даних PNR від авіакомпаній, порівняння даних PNR з відповідними базами даних правоохоронних органів та їх обробку за заздалегідь визначеними критеріями, ідентифікацію осіб, потенційно причетних до терористичного або тяжкого злочину, а також передачу даних PNR національним компетентним органам, Європолу та PIU інших країн ЄС, як спонтанно, так і у відповідь на належно обґрунтовані запити.²²
22. Директива ЄС про PNR також передбачає важливі гарантії захисту даних, а саме: заборону обробки чутливих даних, знеособлення даних через шість місяців, можливість їх повторної персоналізації лише за суворих умов, видалення через п'ять років, а також призначення відповідального за захист даних у кожному PIU та нагляд за діяльністю з обробки даних з боку незалежних національних наглядових органів. Директива ЄС про PNR є найбільш всеосяжним і детальним правовим інструментом в європейському регіоні, що регулює обробку даних PNR.
23. Суд Європейського Союзу ухвалив рішення щодо законності Директиви ЄС про PNR, в якому підкреслив, що Директиву слід розглядати у світлі статей 7 (Повага

18 Рада міністрів ОБСЄ, [MC.DEC/6/16](#), Посилення використання попередньої інформації про пасажирів, стаття 1.

19 Рада Європи, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (CETS № 108), 28 січня 1981 року, ратифікована Україною 30 вересня 2010 року і набула чинності 1 січня 2011 року. [Протокол](#) до неї (CETS № 223) ще не підписаний і не ратифікований Україною.

20 Рада Європи, Конвенція про доступ до офіційних документів (CETS № 205), 18 червня 2009 року, підписана Україною 12 квітня 2018 року, ратифікована Україною 19 серпня 2020 року та набула чинності 1 грудня 2020 року.

21 Європейський Союз, [Директива \(ЄС\) 2016/681 Європейського Парламенту та Ради від 27 квітня 2016 року про використання даних запису реєстрації пасажирів \(PNR\) для запобігання, виявлення, розслідування та переслідування терористичних та тяжких злочинів](#) (далі – Директива ЄС про PNR).

22 Європейська Комісія, [Дані про пасажирів](#).

до приватного та сімейного життя), 8 (Захист персональних даних) та 21 (Недискримінація), а також статті 52(1) (Законність, необхідність та пропорційність обмежень) Хартії основних прав Європейського Союзу, і роз'яснив застосування стандартів необхідності, пропорційності та захисту даних відповідно до права ЄС. Додаткові корисні настанови містить нещодавня Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС.²³ У цьому рішенні Суд ЄС підтвердив, що збір і використання даних PNR має бути строго обмежене боротьбою з терористичними злочинами (визначеними Директивою ЄС 2017/541)²⁴ та тяжкими злочинами (визначеними Директивою про PNR і пов'язаними з організованою злочинністю або злочинами, за які призначається суворе покарання). Нечіткі або занадто широкі визначення тероризму або тяжких злочинів суперечать принципу обмеження мети та роблять непропорційним втручання у приватне життя.²⁵ Що ж до невибіркового збору даних про PNR усіх пасажирів, то він може бути виправданий лише за виняткових обставин, як-от реальна і досить серйозна загроза громадській безпеці. Масовий збір даних про всіх пасажирів без диференціації або конкретного зв'язку з ризиками для громадської безпеки перевищує вимоги пропорційності. У будь-якому разі, масовий збір даних не повинен призводити до постійного, систематичного нагляду за всіма подорожніми.²⁶ Суд ЄС також наголосив, що тривалість зберігання має бути строго необхідною та пропорційною цілям громадської безпеки. Основні вимоги щодо цього включають короткі терміни зберігання для початкового аналізу, зберігання даних протягом короткого, заздалегідь визначеного періоду (6 місяців) перед знеособленням і доступ до даних після знеособлення, чітко пов'язаний з конкретними справами, за наявності судового чи адміністративного дозволу. Понад цей період зберігання даних дозволяється лише в разі, якщо триває розслідування або існує зв'язок з конкретною загрозою, а зберігання незнеособлених даних понад 6 місяців дозволяється лише тоді, коли це суворо виправдано ризиками, пов'язаними з конкретною справою.²⁷ Суд ЄС також постановив, що автоматизована обробка даних PNR є допустимою, але повинна обмежуватися ідентифікацією пасажирів, які можуть бути причетні до терористичної або серйозної злочинної діяльності, і що слід уникати використання дискримінаційних критеріїв (наприклад, на основі «раси»,²⁸ релігії або етнічної належності). Крім того, автоматизовані збіги повинні бути перевірені людиною перш, ніж будуть вжиті правоохоронні заходи, а повністю автоматизоване ухвалення рішень без втручання людини може призвести

23 Європейська рада із захисту даних (ЄРЗД), [Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС C-817/19](#), ухвалена 13 березня 2025 року.

24 Див. деякі коментарі щодо відповідності правам людини визначення «терористичного злочину» в Директиві ЄС 2017/541 про боротьбу з тероризмом в [Аналітичній записці БДППЛ щодо запропонованого перегляду визначення терористичних злочинів у статті 1 Конвенції Ради Європи про запобігання тероризму](#) (2023), зокрема, п. 12.

25 Детальніше див.: Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 141-175; Спеціальний доповідач з питань просування та захисту прав людини і основних свобод в умовах боротьби з тероризмом, Доповідь на 76-й сесії Генеральної Асамблеї, 3 серпня 2021 року, [A/76/261](#), п. 16.

26 Детальніше див.: Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 158-175; D. Lowe, The European Union's Passenger Name Record Data Directive 2016/681: Is it fit for purpose? [Директива ЄС 2016/681 про PNR: Чи відповідає вона заявленій меті?] *International Criminal Law Review* 17 (1), 2017, с. 27.

27 Детальніше див.: Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 214-228; 248-262; Privacy International, Response to Model Legal Provisions [Відповідь на модельні правові норми], 16 листопада 2021 року, с. 4, 6.

28 Автори визнають, що термін «раса» є суто соціальним конструктом, який не має під собою наукового підґрунтя, тому для цілей цього Висновку термін «раса» або «расовий» може використовуватися у посиланнях на міжнародні документи, де зустрічається цей термін, щоби забезпечити охоплення всіх дискримінаційних дій, заснованих на (уявній або фактичній) передбачуваній «расі», походженні, етнічній належності, кольорі шкіри або національності особи – при цьому, як правило, перевага віддаватиметься використанню альтернативних термінів, як-от «національне або етнічне походження»; використання терміну «раса» у цьому Висновку не означає схвалення БДППЛ будь-якої теорії, що ґрунтується на існуванні різних «рас» (див., наприклад, [Практичний посібник БДППЛ із законодавства у сфері боротьби зі злочинами на ґрунті ненависті](#) 2022 року, переглянуте видання, виноска 14 та Розділ 2.3.1 і посилання у ньому).

до порушення права на недоторканність приватного життя та належну правову процедуру.²⁹

24. Щодо передачі даних PNR третім країнам, то останні повинні забезпечити рівень захисту даних, еквівалентний рівню, передбаченому законодавством ЄС. Така передача повинна ґрунтуватися на угодах або рішеннях про достатність у рамках Загального регламенту про захист даних³⁰ і обмежуватись випадками, коли держава-одержувач використовуватиме дані виключно для боротьби з тероризмом або тяжкими злочинами. Угоди про обмін даними з країнами, які не мають надійного захисту або мають нечіткі гарантії, суперечать стандартам захисту даних ЄС.³¹ Перед передачею даних PNR також необхідно оцінити стан дотримання прав людини та захисту даних у третій країні, а також правові гарантії та інституційний контроль і нагляд за діяльністю органу, що отримує такі дані.³² Також має бути чітке зобов'язання не передавати такі дані PNR, які можуть бути використані в цілях, що порушують права людини, наприклад, можуть призвести до катувань або іншого жорстокого поводження, або дозволять країні придушувати свободу слова чи переслідувати правозахисників, або допускати подальші порушення прав людини.³³
25. Особи, чиї дані PNR збираються, повинні мати юридично закріплені права, включаючи право на доступ, виправлення та видалення своїх даних, а також право на ефективний засіб правового захисту в разі порушення; такий засіб повинен бути швидким, практичним, а не теоретичним, доступним (без невинуватених практичних або фінансових бар'єрів) і розглядатися незалежним органом.³⁴ Вони також мають право бути поінформованими про практику обробки даних і повинні мати судові або адміністративні засоби для оскарження незаконної обробки.³⁵ Відсутність доступних прав і засобів правового захисту для пасажирів суперечить зобов'язанням щодо підзвітності та прозорості. Крім того, дані PNR можуть перехресно зв'язатися із заздалегідь визначеними контрольними списками. У такому разі ці списки повинні бути точними, регулярно оновлюватися і базуватися на об'єктивних критеріях, не призводити до профілювання на основі чутливих персональних даних або захищених характеристик (наприклад, «раси», релігії або етнічної належності), а особи повинні мати ефективний механізм для оскарження

29 Детальніше див.: Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 176-181, 202-213.

30 Європейська Комісія має повноваження визначати на підставі статті 45 Регламенту (ЄС) 2016/679, чи забезпечує країна за межами ЄС достатній рівень захисту даних.

31 Детальніше див.: Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 183-192; Privacy International, *Response to Model Legal Provisions* [Відповідь на модельні правові норми], 16 листопада 202 року, с. 5-6; Спеціальний доповідач з питань просування та захисту прав людини і основних свобод в умовах боротьби з тероризмом, *Response to the Call for Input by OHCHR on Privacy in Digital Age* [Відповідь на запит УВКПЛ матеріалів щодо недоторканності приватного життя в епоху цифрових технологій], с. 6-8.

32 Див., наприклад, для порівняння: Спеціальний доповідач ООН з питань просування та захисту прав людини і основних свобод в умовах боротьби з тероризмом, [Збірка оптимальних практичних методів щодо законодавчої та інституційної основи та заходів, які забезпечують дотримання прав людини спеціальними службами в умовах боротьби з тероризмом](#) (2010), Практика 33; див. також БДПЛ, [Керівні принципи щодо протидії загрозам і викликам з боку «іноземних бойовиків-терористів»](#) (2018), с. 43.

33 Див., наприклад, Венеційська комісія, [Звіт про демократичний нагляд за службами радіоелектронної розвідки](#) CDL-AD(2015)011; [Оновлення 2015 року Звіту про демократичний нагляд за службами безпеки 2007 року та Звіту про демократичний нагляд за службами радіоелектронної розвідки](#), CDL-AD(2015)006, п. 75. Див. також Спеціальний доповідач ООН з питань просування та захисту прав людини і основоположних свобод в умовах боротьби з тероризмом, [Збірка оптимальних практичних методів щодо законодавчої та інституційної основи та заходів, які забезпечують дотримання прав людини спеціальними службами в умовах боротьби з тероризмом](#) (2010), Практика 33; та БДПЛ, [Керівні принципи щодо протидії загрозам і викликам з боку «іноземних бойовиків-терористів»](#) (2018), с. 43.

34 Стаття 2 (3) МПГПП (у поєднанні із [Зауваженнями загального порядку № 31](#) Комітету ООН з прав людини, UN Doc. CCPR/C/21/Rev.1/Add.13 (2004)); та стаття 13 ЄКПЛ (і відповідна практика ЄСПЛ; див. [Посібник із практики застосування статті 13 ЄКПЛ](#) станом на лютий 2025 року, особливо пп. 32-55).

35 Детальніше див.: D. Lowe, *The European Union's Passenger Name Record Data Directive 2016/681: Is it fit for purpose?* [Директива ЄС 2016/681 про PNR: Чи відповідає вона заявленій меті?], *International Criminal Law Review* 17 (1), 2017, с. 27; E. Brouwer, *The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?* [Система PNR в Європейському Союзі та права людини: Передача даних про пасажирів чи свобода пасажирів?], 2009, с. 26-28.

свого включення до такого списку.³⁶ Недосконалі або застарілі контрольні списки в поєднанні з неналежним наглядом можуть призвести до хибнопозитивних результатів і невиправданих обмежень свободи пересування.

26. Важливо також розуміти контекст, у якому здійснюється обробка даних PNR, і потенційні наслідки, особливо для управління кордонами. Дані PNR розкривають схеми подорожей пасажирів і, з огляду на великий обсяг зібраної інформації, можуть також розкривати чутливі дані, наприклад, про етнічне походження, політичні погляди, релігію чи переконання або інформацію про здоров'я чи сексуальне життя,³⁷ що може наразити людей на загрозу дискримінації чи інших порушень прав людини, навіть хоча Директива про PNR передбачає, що такі чутливі дані не можуть оброблятися.³⁸ Автоматизована обробка даних PNR може посилити дискримінаційні практики, пов'язуючи особисті риси з конкретними ризиками. Завчасний обмін даними PNR також може призвести до обмеження свободи пересування або завадити людям ефективно шукати притулку. Дані PNR дозволяють державним органам відстежувати осіб, які ймовірно становлять ризик для безпеки країни – на основі автоматизованої обробки їхніх даних. Водночас, до доступу й обробки даних залучені різні державні органи (наприклад, правоохоронні органи, органи прикордонного контролю та митні органи). Тож існує вищий ризик неправомірного використання даних. Наглядовий орган повинен мати чіткий мандат для виконання своїх обов'язків, а також компетентності та повноваження для забезпечення дотримання прав людини. Автоматизована обробка даних PNR може створити додатковий ризик через відсутність прозорості та розуміння роботи автоматизованих систем.
27. До 28 січня 2025 року збір, обробка та обмін даними API регулювалися Директивою Ради 2004/82/ЄС від 29 квітня 2004 року про обов'язок перевізників повідомляти дані про пасажирів (далі – Директива ЄС про API).³⁹ Ця Директива накладає на авіаперевізників зобов'язання до зльоту літака передавати на запит дані API до держави-члена ЄС, до якої прямує рейс. Це стосується вхідних рейсів з третіх країн і має на меті покращити прикордонний контроль. 28 січня 2025 року набули чинності два нових Регламенти, а саме: (i) про збір та передачу API для полегшення контролю на зовнішніх кордонах⁴⁰ (далі – новий Регламент ЄС про API 2025/12 щодо прикордонного контролю) та (ii) про збір і передачу попередньої інформації про пасажирів (API) для запобігання, виявлення, розслідування та переслідування терористичних злочинів і тяжких злочинів⁴¹ (далі – новий Регламент ЄС про API 2025/13 щодо терористичних злочинів і тяжких злочинів), які разом іменуються новими Регламентами ЄС про API. Ці нові регламенти спрямовані на запровадження єдиних вимог до збору даних API перевізниками, підвищення якості даних API, збору даних авіаперевізниками з використанням автоматизованих засобів, обов'язкової передачі даних державам-членам та

36 Детальніше див.: Спеціальний доповідач з питань просування та захисту прав людини і основоположних свобод в умовах боротьби з тероризмом, Консультативна зустріч експертів БДПІЛ з питань прав людини, пов'язаних зі збором та обміном інформацією та новими технологіями в управлінні кордонами в умовах боротьби з тероризмом та свободи пересування, 15 червня 2020 року, с. 3.

37 Рада Європи, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (CETS № 108), стаття 6.

38 Директива ЄС про PNR 2016/681, стаття 13. Див. також БДПІЛ, [Аналітична записка: Управління кордонами та права людини – Збір, обробка й обмін персональними даними та використання нових технологій у контексті боротьби з тероризмом і забезпечення свободи пересування](#) (2021), с. 13.

39 Директива Ради 2004/82/ЄС від 29 квітня 2004 року про обов'язок перевізників передавати дані пасажирів <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0082>>.

40 [Регламент \(ЄС\) 2025/12](#) Європейського Парламенту та Ради від 19 грудня 2024 року про збирання та передачу попередньої інформації про пасажирів для підвищення ефективності та полегшення прикордонного контролю, що вносить зміни до Регламентів (ЄС) 2018/1726 та (ЄС) 2019/817 та скасовує Директиву Ради 2004/82/ЄС.

41 [Регламент \(ЄС\) 2025/13](#) Європейського Парламенту та Ради від 19 грудня 2024 року про збирання та передачу попередньої інформації про пасажирів для запобігання, виявлення, розслідування та переслідування терористичних злочинів і тяжких злочинів та внесення змін до Регламенту (ЄС) 2019/818.

підвищення ефективності передачі даних авіаперевізниками державам-членам, а також на забезпечення повної відповідності правилам ЄС щодо захисту даних.⁴² Вони також роз'яснюють, що правила Директиви ЄС про PNR застосовуються до питань, які конкретно не охоплені новим Регламентом ЄС про API 2025/13 щодо терористичних злочинів і тяжких злочинів, а надто стосовно правил подальшої обробки даних API, отриманих РІУ, обміну інформацією між державами-членами, умов доступу для Європейського поліцейського офісу (Європолу), передачі даних третім країнам, зберігання та знеособлення, а також захисту персональних даних.⁴³

1.2. Захист даних і право на повагу до приватного життя

28. Права людини та основні свободи часто обмежують начебто заради безпеки. Іноді питання прав людини та безпеки сприймають як такі, що знаходяться в обернено пропорційній залежності одне від одного – тобто для підвищення рівня безпеки потрібно зменшити обсяг прав людини, – проте зобов'язання в рамках ОБСЄ з питань людського виміру та підхід ООН полягають у тому, що ефективні заходи безпеки та захист прав людини не суперечать, а підсилюють одне одного.⁴⁴ По суті, повага до прав людини й основних свобод для всіх, до демократії та верховенства права є наріжним каменем схваленої ОБСЄ всеосяжної концепції безпеки⁴⁵ і має лягти в основу будь-якої реформи сектору безпеки.⁴⁶
29. Держави-учасниці ОБСЄ визнали⁴⁷ важливість підходу, орієнтованого на «безпеку людини», за якого права та безпекові потреби людей лежать в основі функцій безпеки. Згідно з цим підходом, головною метою інститутів сектору безпеки є достатнє й ефективне надання послуг усім членам суспільства, незалежно від їх національного чи етнічного походження, політичних або інших переконань, статі, гендерної ідентичності чи сексуальної орієнтації, релігії чи переконань або будь-яких інших ознак.⁴⁸ Сектор безпеки, включаючи правоохоронні органи й органи управління кордонами, підпорядковується тим самим стандартам належного врядування, що й будь-який інший сектор державного управління, і повинен у підзвітний та ефективний спосіб забезпечувати безпеку в рамках демократичного цивільного контролю, верховенства права та поваги до прав людини, в тому числі гендерної рівності.⁴⁹
30. Основні права людини також відіграють значну роль у контексті управління кордонами та збору даних. Варто зазначити, що Резолюція РБ ООН 2396 закликає збирати, обробляти й аналізувати дані API та PNR відповідно до внутрішнього законодавства та міжнародних зобов'язань, а також з повною повагою до прав людини та основних свобод.⁵⁰ Відповідно до Резолюції, використання даних PNR має обмежуватися цілями запобігання, виявлення й розслідування терористичних

42 <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1262>.

43 Див. новий [Регламент ЄС про API 2025/13 щодо терористичних злочинів і тяжких злочинів](#), Розділ 5.

44 БДПІЛ, Інформаційна довідка щодо реагування на транснаціональні загрози та виклики в регіоні ОБСЄ: людський вимір (2012). Див. також Генеральна Асамблея ООН, 15 вересня 2005 року, A/60/L.1, п. 72, і Генеральний секретар ООН Кофі Аннан, Звернення до Ради Безпеки 18 січня 2002 року.

45 ОБСЄ, Стамбульська хартія європейської безпеки (1999), п. 19.

46 ОБСЄ, Хартія про запобігання тероризму та боротьбу з ним, 10-та зустріч Ради міністрів, Порту, 2002, пп. 5-7; та Консолідована концептуальна база ОБСЄ для боротьби з тероризмом, затверджена Рішенням № 1063 Постійної ради на 934-му пленарному засіданні 7 грудня 2012 року (PC.DEC/1063). Див. також ООН, Глобальна контртерористична стратегія і план дій (2006), Компонент IV; та Заяву міністрів ОБСЄ на підтримку Глобальної контртерористичної стратегії ООН (MC.DOC/3/07, 30 листопада 2007 року). Див. також Спільну заяву Верховного комісара ООН з прав людини, Генерального секретаря Ради Європи та Директора БДПІЛ (29 листопада 2001 року).

47 ОБСЄ, Стратегія протидії загрозам безпеці та стабільності у 21 столітті, Маастрихт, 2003.

48 Див., наприклад, Женевський центр демократичного контролю над збройними силами (ДКЗС), БДПІЛ та ООН-Жінки, Підхід до питання про жінок, мир і безпеку в контексті управління сектором безпеки. Концептуальна записка; БДПІЛ, Інформаційна довідка щодо реагування на транснаціональні загрози та виклики в регіоні ОБСЄ: людський вимір (2012), с. 2.

49 Генеральний секретар ОБСЄ, Звіт про підхід ОБСЄ до управління та реформування сектору безпеки (SSG/R) (2019), с. 2.

50 РБ ООН, [S/RES/2396 \(2017\)](#), пп. 11-13.

злочинів.⁵¹ Тож можна дійти висновку, що держави, створюючи законодавчу базу щодо даних API та PNR, повинні дотримуватися своїх зобов'язань поважати та захищати основні права людини, як передбачено міжнародним правом.

1.2.1 Право на повагу до приватного життя

31. Неможливість ефективно здійснювати право на повагу до приватного життя ставить під загрозу повну реалізацію широкого спектру інших прав. Захист персональних даних нерозривно пов'язаний із правом на повагу до приватного життя і є особливо актуальним в контексті обробки даних для цілей управління кордонами, зокрема в контексті боротьби з тероризмом.
32. Право на повагу до приватного і сімейного життя закріплено в ключових міжнародних і регіональних документах, включаючи статтю 17 Міжнародного пакту про громадянські і політичні права⁵² (МПГПП), статтю 8 Європейської конвенції про захист прав людини і основоположних свобод⁵³ (ЄКПЛ) і статтю 7 Хартії основних прав ЄС.
33. Як зазначає Спеціальний доповідач ООН з права на недоторканність приватного життя, «необхідно, щоби держави розробили схему для забезпечення дотримання права на захист персональних даних таким чином, щоби суб'єкти даних отримували інформацію про їх обробку, могли здійснювати належний контроль над своїми даними і в разі порушення могли обрати засіб правового захисту, спрямований на відновлення їхнього права, відшкодування або компенсацію за завдану шкоду, залежно від обставин... Відповідальність держав щодо права на недоторканність приватного життя та захисту даних в епоху цифрових технологій передбачає, окрім утримання від порушення цих прав і їх дотримання, ще й необхідність вжиття позитивних заходів для ефективної реалізації цих прав.»⁵⁴ У сфері збору й обміну даними API/PNR відбувається взаємодія відповідальних органів з суб'єктами приватного сектору, а саме з авіакомпаніями, що вимагає особливої ретельності у виконанні чинних обов'язків щодо дотримання прав на повагу до приватного життя. У зв'язку з цим слід зазначити, що в Рішенні Ради міністрів ОБСЄ № 6/16 держави-учасниці ОБСЄ зобов'язалися створити системи API відповідно до стандартів захисту даних і поваги до приватного життя.
34. Стаття 7 Хартії основних прав ЄС також захищає право на недоторканність приватного життя, що кореспондується зі статтею 8 Європейської конвенції про захист прав людини і основоположних свобод (далі – ЄКПЛ), причому значення та обсяг цього права є однаковими в обох документах. Отже, обмеження, що можуть бути законно накладені на це право, є такими самими, як і ті, що дозволені статтею 8 ЄКПЛ. Втручання у право на повагу до приватного життя є допустимим лише тоді, коли воно відповідає суворим вимогам статті 8 (2) ЄКПЛ, тобто таке втручання має здійснюватися «згідно із законом», переслідувати «законну мету» (як-от захист національної та громадської безпеки чи економічного добробуту країни, запобігання заворушенням чи злочинам, захист здоров'я чи моралі або

51 РБ ООН, [S/RES/2396 \(2017\)](#), пп. 11-13.

52 Міжнародний пакт про громадянські і політичні права (МПГПП), прийнятий Генеральною Асамблеєю ООН резолюцією 2200А (XXI) від 16 грудня 1966 року. Україна здала на зберігання свою ратифікаційну грамоту про ратифікацію МПГПП 12 листопада 1973 року. Стаття 17 Пакту проголошує, що «ніхто не може зазнавати безпідставного або незаконного втручання в його особисте і сімейне життя, безпідставного посягання на недоторканність його житла або таємницю його кореспонденції, а також незаконного посягання на його честь і репутацію».

53 Конвенція Ради Європи (РЄ) про захист прав людини і основоположних свобод набула чинності 3 вересня 1953 року. Україна здала на зберігання свою ратифікаційну грамоту ЄКПЛ на 11 вересня 1997 року.

54 Рада з прав людини Генеральної Асамблеї ООН, [A/HRC/55/46](#). Доповідь Спеціального доповідача з питання про право на недоторканність приватного життя: Правові механізми захисту персональних даних та недоторканності приватного життя в епоху цифрових технологій, 18 січня 2024 року, пп. 12-13.

- захист прав і свобод інших осіб), а також бути «необхідним у демократичному суспільстві» і строго пропорційним переслідуваній меті.
35. В ЄС сам захист даних є правом, що відображено у статті 8 Хартії основних прав ЄС та статті 16 Договору про функціонування Європейського Союзу (далі – ДФЕС). Суд ЄС зазначив, що збір, обробка, зберігання та передача даних API/PNR, як того вимагають резолюція Ради Безпеки 2396 (2017) та резолюція Ради Безпеки 2482 (2019)⁵⁵, самі собою вже є серйозним втручанням у право на недоторканність приватного життя.⁵⁶
36. Втручання у право на повагу до приватного і сімейного життя, захищене, зокрема, статтею 17 МПГПП, статтею 8 ЄКПЛ та статтею 7 Хартії основних прав ЄС, може, однак, бути виправданим за умови, що воно ґрунтується на законі, є необхідним і пропорційним для досягнення законної мети.⁵⁷ Крім того, обмеження має бути недискримінаційним (статті 2 і 26 МПГПП, стаття 14 ЄКПЛ і Протокол № 12 до ЄКПЛ⁵⁸ та стаття 21 Хартії основних прав ЄС).
37. Вимога, щоби втручання ґрунтувалося на законі, полягає не лише в тому, щоб обмеження мало чітку основу в національному законодавстві, але також стосується якості відповідного законодавства, яке має бути чітким, передбачуваним і достатньо доступним.⁵⁹ Таким чином, згадане законодавство має бути достатньо чітким і точним, щоби дозволити особам діяти відповідно до закону, при цьому чітко окреслюючи сферу дискреційних повноважень органів державної влади і надаючи розумні орієнтири щодо того, як ці положення будуть тлумачитися і застосовуватися.⁶⁰ Пропорційність вимагає, щоб обраний захід був доречним, найменш інтрузивним і пропорційним, *строго кажучи*, для досягнення переслідуваної мети. Отже збір, обробка, зберігання та передача даних API/PNR повинні бути відповідними та пропорційними меті боротьби з тероризмом або тяжкими кримінальними злочинами. Закон повинен надавати дозвіл на збір, обробку, зберігання та передачу даних API/PNR компетентними органами; передбачати обмеження мети збору, обробки, зберігання та передачі даних API/PNR вузько визначеними злочинами (строго і точно визначеного) тероризму⁶¹ та тяжкими кримінальними злочинами; гарантувати, що збір персональних даних обмежується тими з них, які безпосередньо стосуються і є необхідними для досягнення визначеної мети; забезпечувати точність, конфіденційність і цілісність даних; регулювати повноваження для уникнення зловживань даними API/PNR; і,

55 РБ ООН, [S/RES/2396 \(2017\)](#), п. 12; і РБ ООН, [S/Res/2482 \(2019\)](#), п. 15.

56 Суд ЄС, [C-817/19 \[GC\]](#), *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 111.

57 Стаття 8(2) ЄКПЛ передбачає: «Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб». Див. також Суд ЄС, [C-817/19 \[GC\]](#), *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 113.

58 Україна ратифікувала Протокол № 12 до ЄКПЛ 27 березня 2006 року, і він набув чинності 1 липня 2006 року.

59 Див., наприклад, Комітет ООН з прав людини, [Зауваження загального порядку № 16: Стаття 17 \(Право на недоторканність приватного життя\)](#). Право на повагу до приватного і сімейного життя, житла і кореспонденції та захист честі і репутації; див. також ЄСПЛ, [Silver and Others v. the United Kingdom](#), по. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 березня 1983 року, п. 87.

60 Див, наприклад, ЄСПЛ, справа [Lebois v. Bulgaria](#), № 67482/14, 19 жовтня 2017 року, пп. 66-67. Див. також, наприклад, Венеційська комісія, [Мірило правовладдя \(Контрольний список запитань для оцінки дотримання верховенства права\)](#), CDL-AD(2016)007, п. 58. Крім того, див. ЄСПЛ, [The Sunday Times v. the United Kingdom \(№ 1\)](#), № 6538/74, де Суд постановив, що «закон повинен бути сформульований з достатньою точністю, щоб дозволити громадянину регулювати свою поведінку, маючи можливість передбачити, що є розумним і які наслідки може спричинити та чи інша дія».

61 Щодо визначення поняття «тероризм» див. [Аналітичну записку БДППЛ щодо запропонованого перегляду визначення терористичних злочинів у статті 1 Конвенції Ради Європи про запобігання тероризму](#) (2023). Пропоноване модельне визначення тероризму на основі цих критеріїв див.: Спеціальний доповідач ООН з питань протидії тероризму, Доповідь Раді ООН з прав людини («Десять елементів передової практики у сфері боротьби з тероризмом»), UN Doc. A/ HRC/16/51, 22 грудня 2010 року, п. 28.

нарешті, передбачати механізми захисту прав суб'єктів даних і забезпечувати доступ до ефективних засобів правового захисту в разі їх порушення.⁶²

1.2.2 Право на захист даних

38. Право на захист даних не є окремим правом відповідно до МПГПП. Водночас Комітет ООН з прав людини роз'яснив, що стаття 17 МПГПП також вимагає, щоби *«кожен мав право в зрозумілій формі з'ясувати, чи зберігаються його персональні дані в автоматизованих файлах даних, і якщо так, то які саме і з якою метою. Кожен також повинен мати можливість з'ясувати, які органи державної влади або приватні особи чи організації контролюють або можуть контролювати його файли. Якщо такі файли містять некоректні персональні дані або були зібрані чи оброблені всупереч положенням закону, кожен повинен мати право вимагати їх виправлення або знищення»*.⁶³ Дві резолюції ООН, ухвалені у 2016 та 2017 роках, також є актуальними, оскільки вони стосуються відповідальності приватного сектору за дотримання прав людини. Резолюції закликають компанії інформувати користувачів про збір, використання, поширення та зберігання персональних даних, а також встановлювати прозорі політики їх обробки.⁶⁴ За словами Спеціального доповідача ООН з права на недоторканність приватного життя, *«обробка персональних даних повинна здійснюватися з повагою та відповідно до низки принципів і вимог, що забезпечить належне поводження з особистою інформацією, гарантуючи, зокрема, право на недоторканність приватного життя та безперешкодний розвиток особистості..... Для досягнення цієї мети суб'єкти даних повинні мати можливість здійснювати контроль над своєю особистою інформацією, саме тому закони про захист даних і недоторканність приватного життя надають їм низку прав»*.⁶⁵ Деякі з цих прав мають особливе значення в контексті збору й обробки даних API/PNR, про що йтиметься нижче.
39. Право на захист персональних даних також не є окремим правом за ЄКПЛ, але ЄСПЛ визнав, що захист персональних даних має фундаментальне значення для реалізації особою свого права на повагу до приватного і сімейного життя, житла і кореспонденції, гарантованого статтею 8 Конвенції.⁶⁶ У своїх рішеннях ЄСПЛ спирається на право на повагу до приватного життя у зв'язку з автоматизованою обробкою персональних даних, закріплене в Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108)⁶⁷ та Протоколі про внесення змін⁶⁸ до неї, які Україна ще не ратифікувала (Конвенція 108 відома також як модернізована Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, далі – модернізована Конвенція 108). Модернізована Конвенція 108 передбачає юридично обов'язкові зобов'язання у сфері захисту даних, має глобальний вимір і горизонтальну сферу застосування,

62 Див. також: Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 141-119-140.

63 Див., наприклад, Комітет ООН з прав людини, [Зауваження загального порядку № 16: Стаття 17 \(Право на недоторканність приватного життя\)](#), Право на повагу до приватного і сімейного життя, житла і кореспонденції та захист честі і репутації, п. 10.

64 ООН, Генеральна Асамблея, Переглянутий проект резолюції про право на недоторканність приватного життя в цифрову епоху, A/C.3/71/L.39/Rev.1, Нью-Йорк, 16 листопада 2016 року; ООН, Рада з прав людини, Право на недоторканність приватного життя в цифрову епоху, A/HRC/34/L.7/Rev.1, 22 березня 2017 року.

65 ООН, Доповідь Спеціального доповідача з питання про прав на недоторканність приватного життя, Правові механізми захисту персональних даних та недоторканності приватного життя в епоху цифрових технологій, A/HRC/55/46, пп. 22-23.

66 Європейський суд з прав людини, Посібник з прецедентного права Конвенції – Захист даних, 31 серпня 2024 року (останнє оновлення), п. 3.

67 Рада Європи, Конвенція про захист осіб у зв'язку з обробкою персональних даних, 28 січня 1981 року. Ратифікована Україною 6 липня 2010 року.

68 Рада Європи, Протокол про внесення змін до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (CETS № 223). Україна не підписала і не ратифікувала цей Протокол.

тобто застосовується до обробки даних як у державному, так і в приватному секторах.

40. Модернізована Конвенція 108 застосовується до всієї обробки даних, що здійснюється як приватним, так і державним сектором, включаючи обробку даних судовими та правоохоронними органами. Відповідно до неї, персональні дані означають *«будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною»*. Такі дані охоплюють не лише інформацію, що безпосередньо ідентифікує «суб'єкта даних» (наприклад, ім'я та прізвище), а й будь-який елемент, що опосередковано ідентифікує особу (наприклад, інтернет-протокол або IP адреса). Відповідно до статті 2 Конвенції 108, «обробка даних» включає *«будь-яку операцію або сукупність операцій, що здійснюються з персональними даними, як-от збирання, зберігання, збереження, зміну, витяг, розкриття, надання, видалення, знищення або проведення логічних та/чи арифметичних операцій з такими даними»*. Вона спрямована на захист суб'єктів даних від зловживань, які можуть виникнути в результаті обробки персональних даних, і регулює транскордонний обмін персональними даними. Відповідно до статті 6 модернізованої Конвенції 108, персональні дані, що розкривають «расове» походження, політичні погляди, релігійні або інші переконання, а також інформацію про здоров'я чи статеве життя особи або про будь-яку судимість, не можуть автоматично оброблятися, якщо національне законодавство не передбачає відповідних гарантій, які доповнюють гарантії Конвенції 108 і які повинні *«захищати від ризиків, які обробка чутливих даних може становити для інтересів, прав та основних свобод суб'єкта даних, зокрема, від ризику дискримінації»* (нова стаття 6(1) і (2) модернізованої Конвенції 108). Інформація, що підпадає під ці категорії, описані як «чутливі», вимагає підвищеного рівня захисту та додаткових гарантій⁶⁹, а автоматична обробка таких чутливих даних *«дозволяється лише тоді, коли в законі закріплені відповідні гарантії»*.
41. Щоб оцінити, чи відповідає певний захід умові *«необхідності в демократичному суспільстві»*, ЄСПЛ перевіряє, чи відповідає цей захід вимогам, переліченим у статті 5 Конвенції 108. Так, він з'ясовує, чи були персональні дані, що піддаються автоматизованій обробці, отримані та оброблені справедливо і законно. Щоб оцінити, чи мало втручання законну мету, Суд аналізує, чи було дотримано вимогу, згідно з якою персональні дані, що піддаються автоматизованій обробці, повинні збиратися для чітких, визначених і законних цілей. ЄСПЛ розглядає, зокрема, чи було дотримано вимог щодо мінімізації обсягу зібраних даних, забезпечення їх точності, достатності, релевантності та ненадмірності відносно цілей, для яких вони обробляються; обмеження тривалості їх зберігання; використання їх для

69 Протокол (CETS: 223), що вносить зміни до Конвенції 108 (або модернізованої Конвенції 108), хоча ще не підписаний і не ратифікований Україною, визначає, що автоматична обробка таких чутливих даних *«дозволяється лише тоді, коли в законі закріплені відповідні гарантії, що доповнюють гарантії [Конвенції]»*, які повинні *«захищати від ризиків, які обробка чутливих даних може становити для інтересів, прав та основних свобод суб'єкта даних, зокрема від ризику дискримінації»* (запропонована нова стаття 6(1) та (2) Конвенції). У Пояснювальній доповіді до Протоколу 223 також наводяться приклади типів додаткових гарантій, які можуть розглядатися окремо чи в різних поєднаннях щодо обробки таких чутливих даних, включаючи пряму згоду суб'єкта даних; закон, що визначає передбачувану мету та засоби обробки або вказує на виняткові випадки, коли обробка таких даних може бути дозволена; зобов'язання щодо дотримання професійної таємниці; заходи, що вживаються за результатами аналізу ризиків (оцінка ризиків перед обробкою повинна визначати, чи є дані захищеними від несанкціонованого доступу до них, їхньої зміни, а також від вилучення або знищення, а також має бути спрямована на забезпечення високих стандартів захисту даних впродовж усієї обробки; така оцінка повинна ґрунтуватися на міркуваннях необхідності та пропорційності, а також на фундаментальних принципах захисту даних у всьому діапазоні ризиків, включаючи фізичну доступність, мережевий доступ до пристроїв і даних, резервне копіювання й архівування даних; див. Конвенцію 108, [Керівні принципи захисту осіб у зв'язку з обробкою персональних даних у перебігу та для цілей політичних кампаній](#) (2021), п. 4.3.5); конкретний і кваліфікований організаційний або технічний захід безпеки; див. [Пояснювальний звіт - CETS 223 - Автоматична обробка персональних даних \(Протокол про внесення змін\)](#), 10 жовтня 2018 року, п. 56.

- цілей, для яких ці дані були зібрані; а також забезпечення прозорості обробки даних.⁷⁰
42. Іншим ключовим принципом є те, що гарантується обмін персональними даними між сторонами Конвенції 108, хоча може бути запроваджено обмеження на обмін інформацією, якщо законодавство держави-одержувача не забезпечує захисту, еквівалентного тому, що існує в державі-відправнику. Конвенція 108 також, серед іншого, регулює обов'язкове створення національних органів нагляду за захистом даних.
43. В ЄС право на захист даних вважається основоположним правом, відмінним від права на недоторканність приватного життя. Стаття 8 Хартії основних прав ЄС не лише посвідчує право на захист даних, але й окреслює основні принципи, пов'язані з ним. У ній зазначено, що обробка даних повинна здійснюватися справедливо, з чітко визначеними цілями та на основі згоди особи або на законній правовій основі. Крім того, особи мають право на доступ до своїх персональних даних і право вимагати їх виправлення, а дотримання цих принципів контролюється незалежним органом.⁷¹
44. Ключовим інструментом захисту даних в ЄС є Загальний регламент про захист даних (далі – GDPR)⁷². Він забезпечує права на захист даних у всіх сферах, за винятком правоохоронної діяльності, яка регулюється Директивою про правоохоронну діяльність 2016/680 (далі – Директива про правоохоронну діяльність).⁷³ Окремо щодо інформації PNR, дані повинні передаватися або оброблятися відповідно до GDPR (див. статтю 21 (2) Директиви про PNR з посиланням на попередника GDPR, а саме Директиву ЄС 95/46/EC), окрім випадків, коли існує мета кримінального правосуддя (тероризм або тяжкі злочини); тоді застосовуються правила Директиви про правоохоронну діяльність.
45. Стаття 5 GDPR встановлює принципи, що регулюють обробку персональних даних. Ці принципи включають законність, добросовісність і прозорість; обмеження мети; мінімізацію даних; точність даних; обмеження зберігання; цілісність і конфіденційність.⁷⁴

70 Європейський суд з прав людини, Посібник з практики застосування Конвенції - Захист даних, 31 серпня 2024 року (останнє оновлення), п. 108.

71 Агентство ЄС з питань основоположних прав, Рада Європи та Європейський наглядовий орган із захисту даних, Посібник з європейського законодавства про захист даних – видання 2018 року, с. 19.

72 Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних, GDPR).

73 Директива ЄС 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування кримінальних злочинів або виконання кримінальних покарань, а також про вільний рух таких даних, OJ L 119, 4 травня 2016 року.

74 Принцип законності детально викладений у статті 6(1), яка вимагає, щоб будь-яка операція з обробки даних ґрунтувалася принаймні на одній із шести правових підстав, наведених у вичерпному переліку (тобто вимога щодо правових підстав виконується, якщо отримано згоду відповідної особи; обробка даних необхідна для виконання договору; обробка даних необхідна, оскільки існує відповідне юридичне зобов'язання; обробка даних необхідна для захисту життєво важливих інтересів; обробка даних необхідна для виконання завдання, що здійснюється в інтересах суспільства / на виконання офіційних повноважень; або обробка даних необхідна для представлення законних інтересів). Значення принципу прозорості витікає з Преамбули 39 GDPR, в якій зазначено, що «фізичні особи повинні бути обізнані про те, що їхні персональні дані збирають, використовують, обговорюють або іншим чином обробляють, а також про те, в якому обсязі ці дані обробляють чи оброблятимуть»; суб'єкти даних повинні бути «поінформовані про ризики, правила, гарантії та права, пов'язані з обробкою... і про те, як користуватися своїми правами»; уся інформація, що їм надається, має бути «доступною та зрозумілою», а також викладеною «чіткою і простою мовою». Принцип обмеження мети, який також закріплений у статті 8 (2) Хартії основних прав ЄС, гарантує, що персональні дані використовуються лише для заявленої та визначеної мети (цілей); обмеження мети має гарантувати, що контролери даних не здійснюють подальшу обробку зібраних даних, якщо така обробка перевищує початкову мету або є несумісною з визначеною метою. Принцип мінімізації даних по суті є принципом пропорційності, оскільки будь-яке втручання в основне право на захист даних має бути пропорційним, а будь-яка обробка персональних даних має бути необхідною. Стаття 5 (1) (e) GDPR вимагає від контролера даних обмежити період збору персональних даних тим, що є строго необхідним для цієї мети. Стаття 5 (1) (d) вимагає, щоб персональні дані були точними і, за необхідності, підтримувалися в

46. У Главі III GDPR викладені права суб'єкта даних, які включають доступ до інформації та її прозорість (статті 13 і 15 GDPR). Тому кожен суб'єкт даних має право на інформацію про обробку його персональних даних будь-яким контролером даних, за винятком обмежених випадків. Інші права суб'єктів даних, особливо актуальні для обробки даних API/PNR, включають право на доступ до власних даних та отримання певної інформації про їх обробку; право на виправлення даних контролером, який обробляє їхні дані, якщо дані є неточними (стаття 16 GDPR); право вимагати від контролера, за необхідності, видалення своїх даних, якщо контролер обробляє їх незаконно (стаття 17 GDPR); право тимчасово обмежити обробку та перенести свої дані до іншого контролера за певних умов; право заперечувати проти обробки на підставах, пов'язаних з їхньою конкретною ситуацією, та проти використання їхніх даних для цілей прямого маркетингу (стаття 21 GDPR). Стаття 25 GDPR встановлює ідею захисту даних «за призначенням і за замовчуванням». Це вимагає від контролерів вжити відповідних технічних та організаційних заходів, призначених для реалізації принципів захисту даних. Це означає, що під час програмування, проєктування та концептуалізації систем і програм, а також придбання систем і послуг у третіх осіб контролер повинен забезпечити врахування захисту даних і належну інтеграцію принципів GDPR у діяльність з обробки даних. Коли певна операція обробки (або сукупність операцій зі схожими характеристиками) становить високий ризик для прав і свобод фізичних осіб, передбачено оцінювання впливу на захист даних (DPIA) (стаття 35 GDPR). Суб'єкти даних також мають право подати скаргу до наглядового органу та право на ефективний судовий захист. Ключовим правом суб'єктів даних є право не бути об'єктом рішень, заснованих виключно на автоматизованій обробці, включаючи профілювання, які мають юридичні наслідки або які суттєво впливають на нього або неї. Інші права включають право на втручання людини в обробку даних з боку контролера, висловлення своєї позиції та оскарження рішення, що ґрунтується на автоматизованій обробці. ЄСПЛ також визнає деякі з цих прав у своїй практиці.⁷⁵
47. Суд ЄС розглядав питання про правила захисту даних, які застосовуються до автоматизованої обробки даних PNR у справі *Ligue des droits humains*.⁷⁶ Як зазначалося вище, Директива ЄС про PNR дозволяє авіакомпаніям ділитися даними PNR з державними органами (правоохоронними органами) виключно з метою боротьби з тероризмом та іншими тяжкими злочинами (стаття 1(2) Директиви ЄС про PNR).
48. Суд ЄС постановив, що GDPR застосовується до обробки персональних даних відповідно до національного законодавства, яке імплементує Директиву про API та Директиву про PNR, охоплюючи як приватних операторів, так і органи державної влади. Однак його норми не поширюються на обробку даних, яку здійснюють підрозділи з питань інформації про пасажирів (PIU) або державні органи, уповноважені запобігати, виявляти, розслідувати та переслідувати терористичні та тяжкі злочини. До того ж, збір та передача даних PNR від суб'єктів приватного сектору відповідним державним органам, як-от PIU, повинні відповідати вимогам

актуальному стані, а також щоб було вжито всіх розумних заходів для негайного видалення або виправлення неточних даних. Принцип обмеження терміну зберігання вимагає, щоб обробка даних була обмежена в часі (Преамбула 39 GDPR передбачає, що «для того, щоб гарантувати, що персональні дані не зберігаються довше, ніж це необхідно, контролер повинен встановити часові межі для видалення або періодичного перегляду»). Принцип конфіденційності та цілісності детально описаний у статті 32 GDPR.

75 Європейський суд з прав людини, Посібник з практики застосування Конвенції – Захист даних, 31 серпня 2004 року (останнє оновлення), глава II.B.

76 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року.

GDPR.⁷⁷ Будь-які винятки, як-от зазначені в статті 23(1)(f) GDPR (що охоплює передачу даних для запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань, включаючи забезпечення громадської безпеки), повинні тлумачитися відповідно до права на недоторканність приватного життя (стаття 7) та захисту персональних даних (стаття 8), гарантованих Хартією основних прав ЄС. Крім того, за Директивою про PNR, PIU та інші правоохоронні органи повинні поводитися з переданими персональними даними відповідно до стандартів GDPR, за винятком випадків, коли обробка пов'язана з цілями кримінального правосуддя (наприклад, тероризм або тяжкі злочини) і коли переважну силу мають правила Директиви про правоохоронну діяльність. PIU здійснюють обробку персональних даних на підставі конкретних запитів компетентних органів. Щодо обробки даних API, то в рішенні Суду ЄС зазначено, що Директива про правоохоронну діяльність не застосовується. Позаяк основною метою збору даних API є прикордонний контроль, усі операції, пов'язані з обробкою цих даних, повинні регулюватися нормами GDPR. Директива про правоохоронну діяльність стає актуальною лише тоді, коли дані API використовуються в правоохоронних цілях, як це визначено в національному законодавстві (стаття 6(1) Директиви про API).

49. Відповідно до статті 47 Хартії основних прав ЄС, особи мають право на ефективний засіб правового захисту, якщо порушено їхні права на захист даних. Це означає, що особи можуть оскаржувати рішення, ухвалені контролерами даних, і домагатися відшкодування, включаючи компенсацію за завдані збитки.
50. За словами Спеціального доповідача ООН з питання про право на недоторканність приватного життя, різні міжнародні та регіональні документи зумовлюють цілу низку прав на захист даних. Ці права включають право на інформацію, право на доступ, право на виправлення, право на оновлення інформації на цифрових носіях, право на видалення, право на забуття, право на обмеження обробки, право на перенесення даних, право на заперечення, право не бути об'єктом рішення, заснованого на автоматизованій обробці, включаючи профілювання, і право на цифровий заповіт.⁷⁸ Спеціальний доповідач ООН також розробив комплекс керівних принципів, що базуються на модернізованій Конвенції 108 та резолюції 45/95 Генеральної Асамблеї⁷⁹ на додаток до GDPR, які включають принципи законності, правомірності та легітимності, згоди, прозорості, мети, справедливості, пропорційності, мінімізації, якості, відповідальності та безпеки.⁸⁰

1.2.3 Потенційний вплив на інші права людини й основоположні свободи

51. Збір, обробка й обмін персональними даними, що містяться в наборах даних API та PNR, здатних впливати на ухвалення рішень на міжнародних кордонах, також можуть призвести до порушення інших прав людини.⁸¹ Неправильні або невідповідні записи в даних API або PNR можуть вплинути на право особи на свободу пересування й інші права. Стаття 12 МПГПП гарантує кожному право залишати будь-яку країну, включаючи свою власну, і право в'їжджати до своєї

77 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 83-84.

78 ООН, A/HRC/55/46, Доповідь Спеціального доповідача з права на приватність – Правові механізми захисту персональних даних та недоторканності приватного життя в епоху цифрових технологій, 18 січня 2024 року.

79 Під назвою «Керівні принципи регулювання комп'ютеризованих файлів персональних даних».

80 ООН, Записка Генерального секретаря, A/77/196*, Право на недоторканність приватного життя – Доповідь, підготовлена Спеціальним доповідачем з питання про право на недоторканність приватного життя, 20 липня 2022 року.

81 Наприклад, БДПІЛ, [Аналітична записка: Управління кордонами та права людини – Збір, обробка й обмін персональними даними та використання нових технологій у контексті боротьби з тероризмом і забезпечення свободи пересування](#) (2021).

країни.⁸² При тому, що в'їзд негромадянина на територію держави може бути обмежений, будь-які обмеження повинні відповідати міжнародним зобов'язанням у сфері прав людини та враховувати інші права, як-от недискримінація, заборона жорстокого, нелюдського або такого, що принижує гідність, поводження та повага до сімейного життя.

52. Залежно від того, як дані API/PNR впливають на потенційні рішення, ухвалені у сфері управління кордонами та безпеки, вони також можуть прямо чи опосередковано впливати на права осіб з особливими потребами у захисті, як-от біженці та шукачі притулку, діти та жертви торгівлі людьми. Необхідно дотримуватися принципу найкращого забезпечення інтересів дитини (див. статтю 3 Конвенції про права дитини). Слід уникати використання даних PNR як заходу імміграційного контролю. Право шукати притулок і користуватися ним закріплено в статті 14 Загальної декларації прав людини (ЗДПЛ) і розвинуто в Конвенції про статус біженців 1951 року і Протоколі до неї.⁸³ Передбачена Конвенцією міжнародна система захисту встановлює основні права біженців і пов'язані з ними зобов'язання держав, включаючи заборону примусового повернення в країну, де їхньому життю або свободі загрожує небезпека (недопущення примусового вислання).⁸⁴ Держави не повинні повертати осіб, які не є їхніми громадянами, до країни, де існує реальний ризик того, що ця особа може бути піддана катуванням або іншим жорстоким, нелюдським або таким, що принижують гідність, видам поводження і покарання,⁸⁵ ризик порушення права на життя⁸⁶ або на особисту недоторканність чи свободу,⁸⁷ кричущого порушення щодо свавільного позбавлення волі,⁸⁸ насильницького зникнення,⁸⁹ ризику явно несправедливого судового розгляду,⁹⁰ серйозних форм сексуального та гендерно зумовленого

82. Право залишати будь-яку країну може підлягати певним обмеженням, але лише тією мірою, якою ці обмеження передбачені законом, є необхідними, пропорційними та недискримінаційними; щодо права повертатися до своєї країни МПГПП також підкреслив, що поняття «своя країна» є ширшим за поняття «країна громадянства» і охоплює також осіб, які не є громадянами, але мають особливі зв'язки з країною, наприклад, довгострокових резидентів; див. Комітет ООН з прав людини, [Зауваження загального порядку № 27: Стаття 12 \(свобода пересування\)](#), UN Doc. CCPR/C/21/Rev.1/Add.9, 2 листопада 1999 року, п. 20. Див. також Зобов'язання ОБСЄ щодо свободи пересування, Відень, 1989, п. 20.
83. Конвенція про статус біженців (1951), ухвалена Конференцією повноважних представників ООН у справах біженців та осіб без громадянства, що проходила в Женеві з 2 по 25 липня 1951 року. Україна приєдналася до Конвенції 10 червня 2002 року.
84. Стаття 33 Конвенції про статус біженців. Принцип недопущення примусового повернення також закріплений у міжнародному праві прав людини, яке забороняє повернення будь-кого в будь-яку країну, де йому чи їй може загрозовувати небезпека катувань або інших серйозних порушень прав людини. Абсолютна заборона катувань тягне за собою абсолютну заборону примусового повернення з метою застосування катувань за будь-яких обставин. Для ознайомлення див. УВКПЛ [«Принцип недопущення примусового повернення в міжнародному праві прав людини»](#).
85. Див.: ООН, [Конвенція проти катувань та жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання](#) (ухвалена 10 грудня 1984 року, набула чинності 26 червня 1987 року, [Україна ратифікувала КПП ООН 24 лютого 1987 року](#)), 1465 UNTS 85, стаття 3; [Міжнародна конвенція про захист усіх осіб від насильницьких зникнень](#) (ухвалена 20 грудня 2006 року, набула чинності 23 грудня 2010 року, Україна приєдналася до КПП 14 серпня 2015 року), 2716 UNTS 3, стаття 16; статті 2(1) та 7 МПГПП (див.: [Зауваження загального порядку № 20 \(1992\)](#), п. 9, який указує на те, що це зобов'язання відображено у статті 7 МПГПП, тоді як [Зауваження загального порядку № 31 \(2004\)](#), UN Doc. CCPR/C/21/Rev.1/Add.13, п. 12, визнає принцип недопущення примусового повернення, закріплений у статті 2 МПГПП). Див. також, наприклад, п. 31 [Зауваження загального порядку № 36 до Пакту про громадянські і політичні права](#) 2018 року.
86. Наприклад, Спеціальний доповідач ООН з питання просування та захисту прав людини й основних свобод в умовах боротьби з тероризмом, [Щорічна доповідь: Десять елементів передового досвіду у сфері боротьби з тероризмом](#), UN Doc. A/HRC/16/51, 22 грудня 2010 року, пп. 38 і Практика 10.5; і Генеральний секретар ООН, [Доповідь про захист прав людини і основних свобод в умовах боротьби з тероризмом](#), A/63/337, 28 серпня 2008 року, п. 45. Див. також УВКПЛ, [Технічна записка щодо принципу невисилки за міжнародним правом прав людини](#) (2018), с. 1; та КПП, [Зауваження загального порядку № 31 \(2004\)](#), п. 12.
87. Там само, п. 45 (Доповідь Генерального секретаря ООН 2008 року); та с. 1 (Технічна записка УВКПЛ щодо невисилки 2018 року).
88. Див., наприклад, Європейський суд з прав людини, [Othman \(Abu Qatada\) v. United Kingdom](#), no. 8139/09, 17 січня 2012 року, п. 233.
89. Див. статтю 16 Міжнародної конвенції про захист усіх осіб від насильницьких зникнень, ухвалені Генеральною Асамблеєю ООН, Резолюція A/RES/61/177 від 20 грудня 2006 року (яка набула чинності 23 грудня 2010 року, Україна приєдналася до Конвенції 14 серпня 2015 року).
90. Генеральний секретар ООН, [Доповідь про захист прав людини та основоположних свобод в умовах боротьби з тероризмом](#), A/63/337, 28 серпня 2008 року, п. 45; та УВКПЛ, [Технічна записка щодо принципу невисилки за міжнародним правом прав людини](#) (2018), с. 1. Див. також Європейський суд з прав людини, [Othman \(Abu Qatada\) v. United Kingdom](#) (Заява № 8139/09, 17 січня 2012 року), пп. 258-262.

насильства,⁹¹ тривалого одиночного ув'язнення⁹² або інших серйозних порушень прав людини⁹³. На додаток до своїх зобов'язань щодо недопущення примусового повернення згідно з міжнародним біженським правом і правом прав людини, держави-учасниці повинні також урахувати положення Протоколу ООН 2000 року про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності⁹⁴ (далі – Палермський протокол ООН), відповідно до захисного застереження, передбаченого в статті 14 (1) для жертв торгівлі людьми.

2. ПЕРЕДУМОВИ

53. Як зазначалося вище, проєкт Закону розроблено в рамках комплексної оцінки транспозиції правових стандартів Європейського Союзу в законодавство України.
54. Стаття 7 Закону України «Про боротьбу з тероризмом» уповноважує Антитерористичний центр при Службі безпеки України координувати на національному рівні виконання резолюцій Ради Безпеки ООН з питань боротьби з міжнародним тероризмом, співробітництво зі спеціальними службами, правоохоронними органами іноземних держав та міжнародними організаціями з питань боротьби з тероризмом та обмін наявною інформацією про пасажирів міжнародних рейсів.
55. З метою імплементації вищезазначеного положення Службою безпеки України спільно з іншими інституціями сектору безпеки і оборони та міжнародними партнерами, у тому числі Програмою підтримки України ОБСЄ, розроблено проєкт Закону України «Про використання інформації про пасажирів для протидії тероризму, тяжким та особливо тяжким злочинам».

3. ЗБІР, ОБРОБКА ТА ОБМІН ДАНИМИ API/PNR

3.1. Обмеження мети

56. Стаття 2 проєкту Закону визначає мету збору даних API та PNR. Дані API збираються для покращення прикордонного контролю та боротьби з «незаконною міграцією»,⁹⁵ тоді як дані PNR отримуються з метою протидії міжнародному тероризму та іншим «тяжким» і «особливо тяжким» злочинам. Новий Регламент ЄС про API 2025/13 має на меті встановити чіткі, гармонізовані й ефективні правила на рівні Союзу щодо збирання та передачі даних API з метою запобігання,

91 Там само, с. 1 (Технічна записка УВКПЛ щодо невисилки 2018 року). Див. також, наприклад, Комітет КПП ООН, [Njamba and Balikosa v. Sweden](#), Повідомлення № 322/2007, 3 червня 2010 року, п. 9.5; та . 9.5; та Комітет КЛДЖ, [Загальна рекомендація № 32](#) (2014), п. 23.

92 Генеральний секретар ООН, [Доповідь про захист прав людини та основоположних свобод в умовах боротьби з тероризмом](#), A/63/337, 28 серпня 2008 року, пп. 39 і 42; і там само, с. 1 (Технічна записка УВКПЛ щодо невисилки 2018 року). Див. також, наприклад, МПГПП, [Зауваження загального порядку № 20](#) (1994), п. 6.

93 Комітет ООН з прав людини, [Kindler v. Canada](#), Повідомлення № 470/1991, п. 13.2: «Якщо держава-учасниця видає особу, яка перебуває під її юрисдикцією, за таких обставин, що в результаті цього існує реальний ризик того, що її права, передбачені Пактом, будуть порушені в іншій державі, держава-учасниця може сама порушувати Пакт»; та [ARJ v. Australia](#), UN Doc. CSCR/C/60/D/692/1996, 11 серпня 1997 року, п. 6.9, де йдеться про ризик будь-якого серйозного порушення прав людини, що призводить до виникнення зобов'язань щодо недопущення примусового повернення.

94 [Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї](#) (далі – Палермський протокол), що доповнює Конвенцію ООН проти транснаціональної організованої злочинності. Протокол затверджений резолюцією 55/25 Генеральної Асамблеї ООН від 15 листопада 2000 року.

95 Для цілей цього Висновку термін «незаконна/нелегальна міграція» використовується в лапках для позначення термінології, що використовується в Директивах та Регламентах ЄС, хоча слід зазначити, що використання слова «нелегальна», коли йдеться про мігрантів, негативно впливає на сприйняття мігрантів широкою громадськістю, ризикуює легітимізувати політику, яка не відповідає гарантіям прав людини, і сприяє ксенофобії та дискримінації (див., наприклад, [Рада Європи, Експертна рада з питань законодавства про НУО, Використання кримінального права для обмеження роботи НУО, що надають підтримку біженцям та іншим мігрантам у державах-членах РС](#) (2019), п. 131 (iii)).

- виявлення, розслідування та переслідування терористичних злочинів і тяжких злочинів, водночас чітко зазначаючи, що Регламент не дозволяє збирати або передавати дані API про польоти в межах ЄС з метою боротьби з «нелегальною імміграцією».⁹⁶
57. Використання даних API, передбачене проєктом Закону, загалом відповідає міжнародним стандартам (прикордонний контроль та протидія незаконній міграції),⁹⁷ хоча для узгодження з новим Регламентом ЄС про API 2025/13 необхідно додати мету запобігання, виявлення, розслідування та переслідування терористичних злочинів і тяжких злочинів. Тоді буде також чітко зазначено, що збір або передача даних API про польоти в межах ЄС з метою боротьби з «нелегальною імміграцією» заборонені.
58. Водночас, мета обробки даних PNR, передбачена проєктом Закону, сформульована ширше, ніж це рекомендовано міжнародними стандартами. Відповідно до згаданих вище Резолюцій РБ ООН, дані PNR мають оброблятися лише для розслідування *терористичних* злочинів та протидії їм. Стандарти Додатку 9 до Чиказької конвенції та Директиви ЄС про PNR розширили цю сферу, включивши до неї «тяжкі злочини», причому Директива містить конкретний перелік тяжких злочинів, для розслідування яких можуть оброблятися дані PNR.⁹⁸ Новий Регламент ЄС про API 2025/13 містить перехресне посилання на перелік тяжких злочинів, наведений у Додатку 2 до Директиви ЄС про PNR. Проєкт Закону також передбачає обробку даних PNR для протидії «*переміщенню осіб, причетних до терористичної діяльності*» (стаття 2). Таке формулювання є досить проблематичним і розпливчастим, що підвищує ризик використання даних PNR для загального імміграційного контролю, а це не відповідатиме міжнародним стандартам. **Рекомендовано узгодити з міжнародними стандартами мету збору даних PNR, а саме з метою запобігання, виявлення, розслідування та переслідування виключно терористичних злочинів та тяжких злочинів, щоби не допустити непропорційного збору даних та їх використання як інструменту масового спостереження, що виходить за межі цілей, визначених міжнародними стандартами.** При тому, що це питання не є об'єктом аналізу в цьому Висновку, важливо також забезпечити чітке визначення відповідних кримінальних правопорушень згідно з міжнародними стандартами у галузі прав людини, суворо обмежуючи кожен із елементів складу зазначених тяжких злочинів, щоби виключити можливість довільного застосування та перевищення сфери дії закону.⁹⁹
59. Більше того, Суд ЄС у своєму рішенні у справі *Ligue des droits humains* постановив, що держави-члени ЄС повинні забезпечити, щоб імплементація ними Директиви про PNR на національному рівні була ефективно обмежена боротьбою з терористичними злочинами та тяжкими злочинами, що «*мають об'єктивний зв'язок, навіть якщо він є лише опосередкованим, з перевезенням пасажирів повітряним транспортом*».¹⁰⁰ Вона не повинна застосовуватися для боротьби зі

96 Див. новий [Регламент \(ЄС\) 2025/13 про збирання та передачу попередньої інформації про пасажирів для запобігання, виявлення, розслідування терористичних злочинів і тяжких злочинів](#), пп. 4 і 32.

97 У Нідерландах Королівська військова і прикордонна поліція, завданням якої є перевірка осіб на кордоні та боротьба з нелегальною міграцією, не має доступу до даних PNR. Вона має доступ лише до даних API. Це відповідає Директиві ЄС про PNR, яка дозволяє обробляти дані PNR лише для запобігання, виявлення, розслідування та переслідування терористичних злочинів і тяжких злочинів. Andrew Priestley, Marc Beauvais, International Experience and Good Practices in API/PNR [Міжнародний досвід та належна практика у сфері API/PNR], 2021, с. 26.

98 Директива ЄС про PNR (2016/681), Додаток 2 містить перелік тяжких злочинів.

99 Щодо визначення поняття «тероризм» див. [Аналітичну записку БДПІЛ щодо запропонованого перегляду визначення терористичних злочинів у статті 1 Конвенції Ради Європи про запобігання тероризму](#) (2023).

100 Суд ЄС, [C-817/19](#), [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 157.

звичайними злочинами.¹⁰¹ Для вирішення проблеми обмеження мети, слід уточнити визначення «тяжких та особливо тяжких злочинів» у Статті 1 проєкту Закону і сформулювати його вузько, щоб забезпечити відповідність вимогам конкретності. Слід зазначити, що стаття 3 (9) Директиви ЄС про PNR визначає «тяжкі злочини» як злочини, перелічені в Додатку 2, за які передбачено покарання у вигляді позбавлення волі або тримання під вартою на максимальний строк не менше трьох років. При тому, що проєкт Закону використовує той самий перелік «тяжких злочинів» і уточнює, що це визначення включає злочини, за які передбачено покарання у вигляді позбавлення волі на строк «понад п'ять років (тяжкі) та понад десять років (особливо тяжкі)», він не гарантує, що сфера застосування обмежується тими злочинами, які «*мають об'єктивний зв'язок, навіть якщо він є лише опосередкованим, з перевезенням пасажирів повітряним транспортом*». Для того, щоб установити об'єктивний зв'язок, необхідно мати об'єктивні критерії для встановлення зв'язку між даними PNR та протидією тяжким злочинам і терористичним злочинам. Тоді як прямий зв'язок стосується «злочинів, спрямованих на перевезення пасажирів повітряним транспортом, а також злочинів, вчинених під час або через подорож повітряним транспортом»,¹⁰² непрямий зв'язок охоплює всі ситуації, коли прямого зв'язку немає, але коли тяжкі злочини і терористичні злочини можуть бути попереджені, виявлені, розслідувані або переслідувані за допомогою обробки даних PNR щодо окремих сполучень або рейсів, тобто, зокрема, коли повітряний транспорт використовується як засіб підготовки таких злочинів або уникнення кримінального переслідування.¹⁰³ **Тому рекомендовано скоротити коло кримінальних правопорушень, для яких може здійснюватися обробка даних PNR (і даних API у світлі нового Регламенту ЄС про API 2025/13) відповідно до проєкту Закону, та чіткіше відобразити їх прямий чи опосередкований зв'язок з перевезенням пасажирів повітряним транспортом.**

60. Нарешті, важливо також звернути увагу на питання персональних даних третіх осіб, які можуть збиратися. Такі дані підпадають під дію Директиви про PNR лише тією мірою, якою вони безпосередньо стосуються виконуваного рейсу та відповідного пасажирів, тобто це дані щодо платіжної інформації та платіжної адреси особи, яка придбала квиток від імені пасажирів, якщо вони безпосередньо стосуються рейсу, а також контактні дані батьків або опікунів, які відправляють або забирають неповнолітнього пасажирів без супроводу дорослих.¹⁰⁴ В іншому разі, **всі інші персональні дані третіх осіб після отримання повинні бути негайно та безповоротно видалені Національним контактним пунктом. Рекомендовано доповнити проєкт Закону відповідною нормою.**

РЕКОМЕНДАЦІЯ А.1

Рекомендовано узгодити з міжнародними стандартами мету збору даних PNR, а саме з метою запобігання, виявлення, розслідування та переслідування виключно терористичних злочинів та тяжких злочинів, щоби не допустити непропорційного збору даних та їх використання як

101 Суд Європейського Союзу, Пресреліз № 105/22 <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105en.pdf>

102 Суд ЄС, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 155.

103 Європейська рада із захисту даних (ЄРЗД), *Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС C-817/19*, ухвалена 13 березня 2025 року, п. 9.

104 Європейська рада із захисту даних (ЄРЗД), *Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС C-817/19*, ухвалена 13 березня 2025 року, п. 10. 5.

інструменту масового спостереження, що виходить за межі цілей, визначених міжнародними стандартами.

РЕКОМЕНДАЦІЯ А.2

Включити до проекту Закону положення про негайне та безповоротне видалення Національним контактним пунктом інших персональних даних третіх осіб після їх отримання.

3.2. Збір та обробка даних API/PNR

61. Єдине вікно даних про пасажирів – це інструмент, який дозволяє сторонам, що беруть участь у пасажирських перевезеннях повітряним транспортом, подавати стандартизовану інформацію про пасажирів, як-от API/PNR, через єдину точку введення даних для виконання всіх регуляторних вимог щодо в'їзду та/чи виїзду пасажирів, які можуть бути встановлені різними державними органами чи відомствами. Концепція «єдиного вікна» покладає на органи влади відповідальність за управління «єдиним вікном» і забезпечення того, щоби залучені органи влади або відомства мали доступ до інформації або фактично отримували інформацію від органу управління «єдиним вікном». Це усуває необхідність для подорожнього чи перевізника подавати ті самі дані до кількох різних органів прикордонного контролю в межах однієї держави.
62. Стаття 5 проекту Закону уповноважує централізовану систему «єдиного вікна» передавати дані API до Національного центру, а дані PNR – до Національного контактного пункту (який є підрозділом з питань інформації про пасажирів, або «PIU» у термінах статті 4 Директиви ЄС про PNR). Порядок функціонування «єдиного вікна» визначається кількома органами, включаючи центральний орган виконавчої влади, що реалізує державну політику у сфері охорони державного кордону, Антитерористичний центр при Службі безпеки України та центральний орган виконавчої влади, що реалізує державну політику у сфері цивільної авіації та використання повітряного простору України, у встановленому законодавством порядку. При тому, що цей підхід, як видається, відповідає Стандартам 9.1 та 9.1.1 Додатку 9 до Чиказької конвенції, таке формулювання є невичерпним і не вимагає запровадження необхідних правових гарантій, зокрема того, що будь-яка процедура, встановлена для «єдиного вікна», відповідає стандартам кібербезпеки та поважає право пасажирів на недоторканність приватного життя. **Рекомендовано посилити це положення, передбачивши вимогу відповідності системи «єдиного вікна» стандартам захисту кібербезпеки.**
63. Статті 8 та 13 проекту Закону стосуються збору даних API та PNR відповідно. Складові даних PNR значною мірою збігаються з тими, що перелічені в Директиві ЄС про PNR. Єдина відмінність між ними полягає в тому, що проект Закону вимагає надати ідентифікаційний номер бронювання, тоді як у Директиві ЄС про PNR така вимога відсутня. Натомість Директива ЄС про PNR передбачає подання так званого «локатора» PNR. По-друге, проект Закону вимагає надання детальної інформації про оплату квитка, але не включає адресу для виставлення рахунку, яка вимагається виключно Директивою ЄС про PNR. Статті 8 та 13 містять поля даних (наприклад, платіжні реквізити), які можуть бути надмірними з огляду на стандарт 9.22 Додатку 9 до Чиказької конвенції, який вимагає мінімізації даних. Водночас варто зазначити, що Суд ЄС розглядав питання про те, чи відповідають поля даних

Директиви ЄС про PNR вимогам чіткості та точності, і постановив, що поля даних, які збираються згідно з Директивою про PNR, в цілому є достатньо чіткими та точними за своєю природою. Разом із тим, він указав, що певні поля даних (а саме інформація щодо виставлення рахунків/платежів, програм для постійних авіапасажирів, а також «загальні зауваження») необхідно тлумачити відповідно до конкретних міркувань, викладених у рішенні *Ligues des droits humains*.¹⁰⁵ **Менше з тим, рекомендовано забезпечити, щоби збір даних обмежувався лише тими даними, які є строго необхідними для запобігання, виявлення, розслідування та переслідування тероризму та тяжких злочинів відповідно до принципу мінімізації даних, а також передбачити чітке положення про обов'язок негайного та безповоротного видалення даних, які виходять за межі встановлених у проекті Закону категорій.**

64. Відповідно до статті 6 (1) Директиви ЄС про PNR, авіакомпанії можуть збирати певну інформацію для надання своїх послуг (наприклад, запити на особливі види харчування – халяльне м'ясо, кошерна їжа – або запити на спеціальне медичне обладнання – інсулінова помпа, кисневий балон тощо), яка містить «чутливі дані», що потенційно розкривають етнічне/«расове» походження, релігійні переконання чи стан здоров'я, і тому не повинні оброблятися як частина даних PNR. **Така інформація має бути негайно та безповоротно видалена, тож слід доповнити проект Закону відповідним положенням.**¹⁰⁶

РЕКОМЕНДАЦІЯ В.

Забезпечити, щоби збір даних обмежувався лише тими даними, які є строго необхідними для запобігання, виявлення, розслідування та переслідування тероризму та тяжких злочинів відповідно до принципу мінімізації даних, а також передбачити чітке положення про обов'язок негайного та безповоротного видалення даних, які виходять за межі встановлених у проекті Закону категорій, у тому числі будь-яких чутливих даних.

3.3. Автоматизована обробка

65. Відповідно до статті 18 проекту Закону, внесені до Національної системи обробки PNR дані, автоматично зв'язуються з відповідними даними автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателями (адміністраторами) яких є державні органи чи оператори і доступ до яких має Національний контактний центр. Цей орган є підрозділом з питань інформації про пасажирів, або «PIU» у термінах Директиви ЄС про PNR, згідно з якою PIU відповідає за збір даних PNR від авіакомпаній, зв'язання даних PNR з відповідними базами даних правоохоронних органів та їх обробку за заздалегідь визначеними критеріями з метою виявлення осіб, потенційно причетних до терористичного злочину або тяжкого злочину, а також передачу даних PNR національним компетентним органам, Європолу та PIU інших країн ЄС, як спонтанно, так і у відповідь на належно обґрунтовані запити. Це відповідає визначенню, наведеному

¹⁰⁵ Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 126-140.

¹⁰⁶ Andrew Priestley, Marc Beauvais, *International Experience and Good Practices in API/PNR* [Міжнародний досвід та належна практика у сфері API/PNR], 2021 р., с. 39

в статті 1 проекту Закону. Стаття 18 також передбачає, що збіги, отримані в результаті попереднього автоматизованого порівняння, підлягають обов'язковій індивідуальній перевірці працівниками Національного контактного пункту.¹⁰⁷ Далі уточнено, що обробка персональних даних здійснюється з дотриманням вимог Закону України «Про захист персональних даних».

66. Важливо, що проект Закону містить додаткові та достатні гарантії щодо автоматизованої обробки даних. Директива ЄС про PNR вимагає, щоби *«...компетентні органи не ухвалювали жодних рішень, які мають несприятливі правові наслідки для особи або суттєво впливають на особу лише через автоматизовану обробку даних про персональні дані,»* і щоби такі *«рішення не ухвалювалися на підставі расової чи етнічної належності особи, її політичних поглядів, релігійних чи філософських переконань, членства у профспілці, стану здоров'я, статевого життя або сексуальної орієнтації»*.¹⁰⁸ Суд ЄС також зазначив, що автоматизована обробка під час попереднього оцінювання даних PNR повинна бути обмеженою і супроводжуватися низкою запобіжних заходів. Дійсно, високий рівень помилок може бути наслідком того, що автоматизовані системи генерують хибнопозитивні результати, тим самим непропорційно впливаючи на невинних пасажирів.¹⁰⁹
67. Стаття 8 Регламенту ЄС 2025/13 і стаття 21 Хартії основних прав ЄС вимагають, щоби збір і обробка даних про пасажирів авіаперевізниками та компетентними органами не призводили до дискримінації осіб за ознаками статі, раси, кольору шкіри, етнічного чи соціального походження, генетичних особливостей, мови, релігійних чи інших переконань, політичних поглядів, належності до національної меншини, майнового стану, народження, інвалідності, віку чи сексуальної орієнтації.
68. Отже неавтоматизована перевірка має бути спрямована на виключення будь-яких дискримінаційних результатів.¹¹⁰ Проект Закону також має чітко визначати, що Національний контактний пункт (PIU) не повинен передавати результати автоматизованої обробки компетентним органам, якщо після такої перевірки він дійде висновку, що немає нічого, що могло б, відповідно до застосовних правових стандартів, викликати обґрунтовану підозру в причетності до терористичних злочинів або тяжких злочинів щодо осіб, ідентифікованих за допомогою автоматизованої обробки, або якщо є підстави вважати, що така обробка призводить до дискримінаційних результатів.¹¹¹ Держави повинні забезпечити, щоби PIU встановив у чіткий і точний спосіб об'єктивні критерії перевірки, які дозволять співробітникам PIU, відповідальним за індивідуальну перевірку, з одного боку, з'ясувати, чи дійсно позитивний збіг стосується особи, яка може бути причетною до терористичних злочинів або тяжких злочинів, і якщо так, то в якій мірі, а отже, підлягає подальшій перевірці компетентними органами, зазначеними в статті 7 Директиви ЄС про PNR, а також, з іншого боку, пересвідчитись у недискримінаційному характері автоматизованої обробки даних, зокрема,

107 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 152. див. також: Директива ЄС про PNR (2016/681), стаття 6 (5). Директива ЄС про PNR, наприклад, передбачає, що держави-члени ЄС забезпечують, аби будь-який позитивний збіг, отриманий в результаті автоматизованої обробки даних PNR, перевірявся в індивідуальному порядку неавтоматизованими засобами для з'ясування того, чи потрібно компетентному органу вживати заходів відповідно до національного законодавства.

108 Директива ЄС про PNR (2016/681), стаття 7(6).

109 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 106, 123-124.

110 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 203.

111 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 204.

- заздалегідь визначених критеріїв і використовуваних баз даних.¹¹² Там, де це можливо, РІУ повинен віддавати перевагу результатам індивідуальної перевірки, проведеної неавтоматизованими засобами, перед результатами, отриманими за допомогою автоматизованої обробки.¹¹³ Важливо також передбачити «...чіткі та точні правила, здатні забезпечити належне скеровування та підтримку аналізу, що його проводять співробітники, відповідальні за індивідуальну перевірку, з метою забезпечення повної поваги до основних прав, закріплених у статтях 7, 8 та 21 Хартії, і, зокрема, гарантувати єдину адміністративну практику в рамках РІУ з дотриманням принципу недискримінації».¹¹⁴ Нарешті, держави зобов'язані забезпечити, щоби РІУ вели документацію щодо всієї обробки даних PNR, здійсненої у зв'язку з попередньою оцінкою, в тому числі в контексті індивідуальної перевірки неавтоматизованими засобами, задля верифікації законності такої обробки та з метою самоконтролю.¹¹⁵
69. Стандарти ІКАО також містять конкретні гарантії щодо автоматизованої обробки персональних даних.¹¹⁶ Ці стандарти вимагають, щоб автоматизована обробка даних PNR базувалася на об'єктивних, точних, конкретних критеріях, які ефективно вказують на існування ризику, не призводячи до незаконної диференціації, а також щоби рішення, які спричиняють значні несприятливі наслідки, що зачіпають законні інтереси фізичних осіб, не ґрунтувалися виключно на автоматизованій обробці даних PNR.
70. **Рекомендовано забезпечити, щоби стаття 18 проєкту Закону чітко відображала вищезазначені гарантії та вимагала, щоби будь-які заздалегідь встановлені критерії, за якими порівнюються дані PNR, не призводили до незаконної диференціації та забезпечували виключення дискримінаційних результатів.** Крім того, бажано включити до цього положення захисне застереження щодо заяв про надання притулку відповідно до Преамбули Директиви ЄС про PNR, в якій зазначено, що «результати обробки даних PNR за жодних обставин не повинні використовуватися державами-членами як підстава для обходу своїх міжнародних зобов'язань за Конвенцією про статус біженців від 28 липня 1951 року зі змінами, внесеними Протоколом від 31 січня 1967 року, а також не повинні використовуватися для відмови шукачам притулку в безпечному та ефективному законному в'їзді на територію Союзу з метою реалізації їхнього права на міжнародний захист».¹¹⁷

РЕКОМЕНДАЦІЯ С.

Відобразити в статті 18 Законопроєкту, що:

- Неавтоматизована перевірка повинна виключати будь-які дискримінаційні результати

112 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 206.

113 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 208.

114 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 205.

115 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 202-212.

116 Додаток 9 до Конвенції ІКАО, стаття 9.28.

117 Директива ЄС про PNR, Преамбула, п. 21

- Національний контактний пункт не передає компетентним органам результати автоматизованої обробки, якщо за результатами такої перевірки він дійде висновку про відсутність підстав, які могли б відповідно до застосовних правових стандартів викликати обґрунтовану підозру в причетності до терористичних злочинів або тяжких злочинів осіб, ідентифікованих за допомогою автоматизованої обробки, або якщо він має підстави вважати, що така обробка призведе до дискримінаційного результату.
- Національний контактний пункт встановлює в чіткий і точний спосіб об'єктивні критерії перевірки, що дозволяють співробітникам Національного контактного пункту, відповідальним за індивідуальну перевірку, з одного боку, з'ясувати, чи стосується і якщо так, то якою мірою, позитивний збіг тієї особи, яка може бути причетною до терористичних злочинів або тяжких злочинів, а тому має пройти додаткову перевірку з боку компетентних органів, як передбачено Статтею 7 Директиви ЄС про PNR, а з іншого боку, пересвідчитись у недискримінаційному характері автоматизованої обробки даних і, зокрема, заздалегідь встановлених критеріїв і використовуваних баз даних.
- Будь-які заздалегідь встановлені критерії, за якими порівнюються дані PNR, не призводять до незаконної диференціації та забезпечують виключення дискримінаційних результатів.
- До цього положення включено захисне застереження щодо заяв про надання притулку.

3.4. Обмін даними з уповноваженими органами

71. Стаття 19 регулює обмін даними API/ PNR з «уповноваженими органами» в Україні. Проєкт Закону визначає ці органи досить широко (у статті 1), не називаючи жодної конкретної установи. Однак, згідно з Директивою ЄС про PNR, держави повинні затвердити перелік компетентних органів, які мають право запитувати або отримувати від PIU дані PNR або результати обробки цих даних для подальшого вивчення цієї інформації або вжиття відповідних заходів з метою запобігання, виявлення, розслідування та переслідування терористичних злочинів або тяжких злочинів.¹¹⁸ **Тому рекомендовано, щоби проєкт Закону містив чіткий перелік уповноважених органів або в тексті самого проєкту Закону, або в додатку до нього, або ж містив посилання на відповідні законодавчі акти, які регулюють діяльність цих уповноважених органів.**
72. Щодо належно обґрунтованого запиту із зазначенням достатніх підстав від компетентних органів про надання й обробку даних PNR у конкретних випадках з метою запобігання, виявлення, розслідування та переслідування терористичних злочинів або тяжких злочинів, як це передбачено у статті 6(2)(b) Директиви ЄС про PNR, Суд ЄС зазначив, що *«важливо, щоби розкриття даних PNR з метою подальшої оцінки, за загальним правилом, за винятком належним чином обґрунтованої невідкладності, підлягало попередньому розгляду, проведеному або судом, або незалежним адміністративним органом»*.¹¹⁹ Така незалежність є дійсно

118 Директива ЄС про PNR, стаття 7 (1).

119 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 223. Див. також ЄРЗД, *Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС C-817/19*, ухвалена 13 березня 2025 року, пп. 25-26.

важливою, щоби запобігти необмеженому використанню даних для цілей правоохоронної діяльності. Як підкреслює Європейська рада із захисту даних (далі – ЄРЗД), «покладання попереднього розгляду на незалежну посадову особу або співробітника конкретного підрозділу адміністративного органу, який по суті не є незалежним, в принципі не відповідатиме тому, що передбачено в рішенні Суду ЄС щодо незалежності. Те саме стосується і незалежної посадової особи або співробітника конкретного підрозділу в межах органу, залученого до проведення кримінального розслідування».¹²⁰ У проєкті Закону мають бути додатково передбачені механізми незалежної перевірки перед наданням відповіді на належно обґрунтовані запити компетентних органів з метою запобігання, виявлення, розслідування та переслідування терористичних злочинів або тяжких злочинів.

73. Стаття 16 (5) покладає на Національну систему обробки PNR обов'язок фіксувати всі випадки отримання доступу до даних PNR. Однак це положення потребує подальшого доопрацювання. Відповідно до Директиви ЄС про PNR, держави повинні вести облік щонайменше збору, консультацій, розкриття та видалення (даних PNR). Записи про консультації та розкриття повинні включати, зокрема, мету, дату і час таких операцій, а також, наскільки це можливо, особу, яка надавала консультацію або розкривала дані PNR, та особу одержувачів цих даних. Записи повинні використовуватися виключно для цілей верифікації, самоконтролю, забезпечення цілісності та безпеки даних або для цілей аудиту. PIU повинен надавати записи за запитом «національному наглядовому органу».¹²¹ **Відповідно, проєкт Закону, в частині 5 Статті 16, повинен включати детальніший перелік інформації, яку необхідно збирати у зв'язку з доступом до даних PNR.**
74. Стаття 11 (4) проєкту Закону містить посилання на реєстрацію Національною системою обробки API всіх випадків отримання доступу до даних API. При тому, що ведення журналів реєстрації всіх операцій з обробки даних API є доброю практикою, слід детальніше описати порядок ведення журналів. Відповідно до нового Регламенту ЄС про API 2025/13 щодо терористичних злочинів та тяжких злочинів, журнали повинні зазначати дату, час, місце передачі даних API.¹²² Журнали не повинні містити жодних персональних даних, окрім інформації, що дозволяє ідентифікувати співробітника органу, відповідального за обробку даних API. Журнали повинні використовуватися лише для забезпечення безпеки та цілісності даних API та законності обробки, і вони повинні бути доступними для національних органів нагляду за захистом даних.¹²³

РЕКОМЕНДАЦІЯ D

Чітко визначити перелік уповноважених органів у самому проєкті Закону або в додатку до нього, або зробити посилання на відповідне законодавство, яке регулює діяльність цих уповноважених органів, а також розробити механізми незалежної перевірки перед наданням відповіді на належно обґрунтований запит компетентних органів з метою запобігання, виявлення,

120 ЄРЗД, [Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС С-817/19](#), ухвалена 13 березня 2025 року, п. 24.

121 Директива ЄС про PNR, стаття 13 (6).

122 Див. новий [Регламент ЄС 2025/13 щодо терористичних злочинів та тяжких злочинів](#), стаття 17.

123 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0729> Стаття 13

розслідування та переслідування терористичних злочинів або тяжких злочинів.

3.5. Зберігання даних

75. Статті 9 та 17 проєкту Закону стосуються зберігання даних API та PNR відповідно. Згідно зі статтею 9, дані API повинні зберігатися як тимчасові файли, а Національна система обробки попередньої інформації про пасажирів (API) міжнародних рейсів (далі – Національний центр обробки API) повинен видаляти дані протягом 24 годин після передавання. Стаття 9 також передбачає, що авіаперевізники повинні видаляти дані впродовж 24 годин після прибуття повітряного судна. Ці положення відповідають чинній Директиві ЄС про API. Слід зазначити, що нові Регламенти ЄС про API збільшують ці терміни з 24 до 48 годин.¹²⁴
76. Стаття 17 проєкту Закону передбачає зберігання даних PNR упродовж п'яти років після їх отримання. Через шість місяців з моменту надання Національному контактному пункту певні дані мають бути знеособлені. Стаття 17 також містить положення, що дозволяє відхилення від стандартних строків, як це передбачено у Додатку 9 до Чиказької конвенції, рекомендованих практиках 9.32 та 9.33, якщо це необхідно в перебігу розслідування, переслідування або судового розгляду.¹²⁵ Директива ЄС про PNR розширює вищезазначені підстави, включаючи також запобігання та виявлення терористичних злочинів або тяжких злочинів та зазначаючи, що «Держави-члени повинні забезпечити безповоротне видалення даних PNR після завершення строку, вказаного в параграфі 1. Це зобов'язання не повинне обмежувати випадків, коли конкретні дані PNR передали компетентному органу та використовують у контексті конкретних справ для цілей запобігання, виявлення, розслідування та переслідування терористичних або тяжких злочинів; у таких випадках зберігання даних компетентним органом повинне бути врегульовано національним правом».¹²⁶
77. У регіоні ОБСЄ не існує єдиної політики щодо максимального терміну зберігання даних API або PNR. Консультативний комітет Конвенції 108 наголосив, що періоди зберігання даних повинні бути чітко визначені й обмежені тим, що є строго необхідним для досягнення поставленої мети. Комітет визнав, що знеособлення даних пасажирів після певного періоду може зменшити деякі ризики, пов'язані з тривалим зберіганням, проте він нагадав, що такі знеособлені дані все ще можуть дозволити ідентифікувати особу. Як наслідок, ці дані залишаються персональними даними і повинні підпадати під відповідні обмеження щодо їх зберігання, щоби запобігти довготривалому спостереженню. Крім того, збір даних про стан здоров'я разом з іншою особистою інформацією може викликати додаткові занепокоєння щодо дотримання прав людини пасажирів, які здійснюють міжнародні подорожі повітряним, наземним і морським транспортом.¹²⁷

124 Стаття 8 нового Регламенту ЄС про API [2025/12](#) та стаття 6 нового Регламенту [ЄС про API 2025/13](#) щодо терористичних злочинів та тяжких злочинів.

125 Додаток 9 ІКАО - Стаття 9.32

126 Директива ЄС про PNR, Стаття 12 (4)

127 БДПІЛ, Аналітична записка: Управління кордонами та права людини – Збір, обробка й обмін персональними даними та використання нових технологій у контексті боротьби з тероризмом і забезпечення свободи пересування, 2021, с. 14.

78. При тому, що стаття 12 Директиви про PNR передбачає п'ятирічний термін зберігання даних, зберігання даних PNR відповідно до статті 12 не може бути виправданим за відсутності об'єктивного зв'язку між таким зберіганням і цілями, які переслідує Директива про PNR.¹²⁸ У своєму рішенні Суд ЄС підкреслив, що положення про п'ятирічний термін зберігання даних «...у поєднанні зі статтями 7 і 8, а також зі статтею 52(1) Хартії основних прав, повинно тлумачитися як таке, що виключає застосування національного законодавства [...] без розбору до всіх авіапасажирів, у тому числі тих, щодо яких не проводилася ані попередня оцінка [...], ані будь-яка верифікація протягом шестимісячного періоду, вказаного у статті 12 (2) зазначеної Директиви, і жодні інші обставини не виявили існування об'єктивного матеріалу, здатного встановити ризик, пов'язаний з терористичними злочинами або тяжкими злочинами, що мають об'єктивний зв'язок, навіть якщо він є лише опосередкованим, з перевезенням пасажирів повітряним транспортом».¹²⁹ Як наголошує Європейська рада із захисту даних, отже «не можна встановлювати загальний термін зберігання, що виходить за межі початкового періоду в шість місяців», а після початкового періоду в шість місяців «окремні набори даних PNR можуть оброблятися виключно у тому разі, коли для відповідних наборів даних існує об'єктивний матеріал, здатний встановити зв'язок із цілями, що їх переслідує обробка відповідно до Директиви про PNR, і виключно доти, доки така обробка є необхідною і пропорційною».¹³⁰
79. Тож до статті 17 проєкту Закону слід внести зміни, передбачивши загальний строк зберігання у шість місяців, який може бути збільшений до п'яти років за наявності об'єктивних матеріалів, здатних встановити ризик, пов'язаний з терористичними злочинами або тяжкими злочинами, що мають об'єктивний прямий чи опосередкований зв'язок з перевезенням пасажирів повітряним транспортом – зі збереженням вищезазначених винятків. Крім того, слід включити стандартне положення про те, що дані PNR повинні бути видалені після закінчення терміну зберігання.

3.6. Міжнародне співробітництво

80. Стаття 24 проєкту Закону прямо пов'язує обмін даними з міжнародними договорами, ратифікованими Україною. Це впливає зі Стандарту 9.25 Додатку 9 до Чиказької конвенції. Як зазначалося вище, відповідно до законодавства ЄС, передача даних PNR третім країнам повинна забезпечувати рівень захисту даних, еквівалентний рівню, передбаченому законодавством ЄС, ґрунтуватися на угодах або рішеннях про достатність у рамках GDPR, а держави повинні обмежувати передачу даних лише тими випадками, коли держава-одержувач використовуватиме дані виключно для боротьби з тероризмом або тяжкими злочинами. Перед передачею даних PNR вкрай важливо оцінити стан дотримання прав людини та захисту даних у країні-одержувачі, а також правові гарантії та інституційний контроль і нагляд, які регулюють діяльність органу, що отримує такі

128 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 299. Див. також ЄРЗД, [Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС C-817/19](#), ухвалена 13 березня 2025 року, п. 30.

129 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 299.

130 ЄРЗД, [Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС C-817/19](#), ухвалена 13 березня 2025 року, п. 29.

дані.¹³¹ Як зазначалося вище, також має бути чітке зобов'язання не передавати такі дані PNR, які можуть бути використані для цілей, що порушують права людини. Угоди про обмін даними з країнами, які не мають надійного захисту персональних даних і прав людини або мають нечіткі гарантії, суперечать стандартам захисту даних ЄС¹³² та міжнародним зобов'язанням у сфері прав людини загалом.

81. Відсутність таких достатніх стандартів і гарантій захисту даних може стати перешкодою для обміну інформацією між державами-учасниками ОБСЄ. Транскордонний обмін даними PNR може вважатися законним лише за умови дотримання стандартів конфіденційності та захисту даних як у країні-відправнику, так і в країні-одержувачі. Як зазначається в аналітичній записці БДПЛ: Управління кордонами та права людини, *«...обмін даними за таких обставин [відсутності гарантій] не лише підриває стандарти захисту даних, а й може призвести до порушення інших прав людини (наприклад, неправомірного обмеження свободи пересування, дискримінації, незаконного затримання або нелюдського та такого, що принижує гідність, поводження чи покарання), якщо захист прав людини в країні-одержувачі є недостатнім. Це може поставити під загрозу не лише окрему особу, яка подорожує, але і її сім'ю чи близьких»*.¹³³ Обмін цими даними може наразити на особливий ризик біженців і шукачів притулку, якщо в результаті їм не дозволять залишити свою або іншу країну. Тому, розробляючи та впроваджуючи системи API та PNR, держави повинні забезпечити ефективні гарантії дотримання прав людини, щоби захистити людей від неправомірної підозри у причетності до тероризму або інших злочинів.
82. Перш ніж укласти угоди про обмін даними API та PNR, держави повинні переконатися, що у країнах-партнерах, з якими планується обмінюватися такою інформацією, повністю запроваджені та дотримуються гарантії поваги до приватного життя та захисту даних, а також інші гарантії дотримання прав людини.¹³⁴ Такі гарантії для забезпечення еквівалентного захисту даних, якими обмінюються з третіми країнами, не відображені в Статті 24. Тому **рекомендовано доповнити Статтю 24 проєкту Закону положенням про те, що перед укладенням угоди про обмін даними API/PNR або перед обміном такими даними на разовій основі слід провести оцінку стану дотримання іншою стороною прав людини та захисту даних, а також оцінку правових гарантій та інституційного контролю, які регулюють діяльність органу-одержувача, щоби переконатися, що третя країна дотримується еквівалентних стандартів захисту. Така угода також повинна переглядатися з певною регулярністю або за необхідності.**

131 Див., наприклад, для порівняння, Спеціальний доповідач ООН з питання просування та захисту прав людини й основних свобод в умовах боротьби з тероризмом, [Збірка оптимальних практичних методів щодо законодавчої та інституційної основи та заходів, які забезпечують дотримання прав людини спеціальними службами в умовах боротьби з тероризмом](#) (2010), Практика 33; див. також БДПЛ, [Керівні принципи щодо протидії загрозам і викликам з боку «іноземних бойовиків-терористів»](#) (2018), с. 43.

132 Детальніше див.: Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 183-192; Спеціальний доповідач з питань просування та захисту прав людини і основних свобод в умовах боротьби з тероризмом, Відповідь на заклик УВКПЛ про надання інформації про конфіденційність у цифрову епоху, с. 6-8.

133 БДПЛ, [Аналітична записка: Управління кордонами та права людини – Збір, обробка й обмін персональними даними та використання нових технологій у контексті боротьби з тероризмом і забезпечення свободи пересування](#), 2021, с. 15.

134 БДПЛ, [Аналітична записка: Управління кордонами та права людини – Збір, обробка й обмін персональними даними та використання нових технологій у контексті боротьби з тероризмом і забезпечення свободи пересування](#), 2021, с. 15.

РЕКОМЕНДАЦІЯ Е.

Передбачити у Статті 24 проєкту Закону, що перед укладенням угоди про обмін даними API/PNR або перед обміном такими даними на *разовій* основі слід провести оцінку стану дотримання іншою стороною прав людини та захисту даних, а також оцінку правових гарантій та інституційного контролю, які регулюють діяльність органу-одержувача, щоби переконатися, що третя країна дотримується еквівалентних стандартів захисту. Така угода також повинна переглядатися з певною регулярністю або за необхідності.

4. НЕДИСКРИМІНАЦІЯ

83. Дані PNR містять детальну інформацію, яка може розкрити чутливі персональні дані, як-от етнічна належність, політичні погляди, релігія, стан здоров'я або сексуальна орієнтація, що може призвести до дискримінації певних осіб або до порушення їхніх прав людини. Навіть якщо законодавство забороняє обробку чутливих даних, однаково існує ризик, що опосередковано можуть бути зроблені певні висновки, наприклад, висновок про чийсь релігійні переконання на основі уподобань у їжі або про політичні погляди на основі схеми подорожей. Завчасний обмін даними API або PNR також може спричинити обмеження свободи пересування, особливо для політичних дисидентів або шукачів притулку.¹³⁵ Стандарт 9.30 Додатку 9 до Чиказької конвенції передбачає, що держави не повинні використовувати дані PNR, які розкривають «расове» або етнічне походження особи, її політичні погляди, релігійні або філософські переконання, членство в профспілках або дані про її здоров'я, статеве життя або сексуальну орієнтацію, окрім як у виняткових і невідкладних обставинах для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи.
84. Як зазначалося, Директива ЄС про PNR зобов'язує уповноважені органи національної безпеки, підрозділи з питань інформації про пасажирів (PIU), автоматично обробляти дані PNR на основі вже наявних баз даних і так званих «заздалегідь визначених критеріїв» (стаття 6 (3) (a) і (b) Директиви ЄС про PNR). Отже, крім виявлення транскордонного переміщення відомих осіб, дані PNR також використовуються для виявлення ще невідомих загроз шляхом обробки даних про пасажирів за заздалегідь визначеними критеріями, які є специфічними індикаторами ризику. Останні, по суті, є алгоритмами, які містять «*критерії пошуку, засновані на минулих і поточних кримінальних розслідуваннях і оперативних даних, які дозволяють відфільтрувати пасажирів, що відповідають певним абстрактним профілям [...]*».¹³⁶ Ці заздалегідь визначені критерії слугують для «*виявлення осіб, причетних до злочинної або терористичної діяльності, які ще не відомі правоохоронним органам*».¹³⁷ Ці критерії встановлюються PIU та оновлюються на основі нових даних і моделей, наявних у системі. Автоматизована

135 БДПЛ, Аналітична записка: Управління кордонами та права людини – Збір, обробка й обмін персональними даними та використання нових технологій у контексті боротьби з тероризмом і забезпечення свободи пересування, 2021, с. 15.

136 Європейська комісія, Звіт Комісії Європейському парламенту та Раді про перегляд Директиви 2016/681 про використання даних реєстрації пасажирів (PNR) для запобігання, виявлення, розслідування та переслідування терористичних злочинів та тяжких злочинів {COM(2020) 305 final}, 24 липня 2020 року, с. 11, виноска 36.

137 Європейська комісія, Звіт Комісії Європейському Парламенту та Раді про перегляд Директиви 2016/681 про використання даних про імена пасажирів (PNR) для запобігання, виявлення, розслідування та переслідування терористичних злочинів та тяжких злочинів {COM(2020) 305 final}, 24 липня 2020 року, с. 24.

обробка даних має багато наслідків для права на недоторканність приватного життя та права на захист даних, що також було визнано Судом ЄС.¹³⁸

85. Суд ЄС наголосив на пов'язаному з цим ризику дискримінації. Хоча Директива про PNR визнає такі ризики в статті 6 (4), Суд ЄС у справі *Ligues des droits humains* підкреслив, що це положення охоплює як пряму, так і непряму дискримінацію.¹³⁹ Це особливо важливо, оскільки заздалегідь встановлені критерії можуть ґрунтуватися на, здавалося б, невинній особистій інформації, яка, менше з тим, може слугувати непрямим індикатором захищених ознак. Наприклад, адреса особи може бути використана як проксі для визначення її віросповідання, «раси» або етнічного походження. Як зазначалося вище, Суд ЄС постановив, що алгоритми повинні бути цільовими, пропорційними та конкретними – лише так можна забезпечити їхню недискримінаційність.¹⁴⁰ Цей принцип має ширше значення, особливо у сфері міграції. Суд зазначив, що високий рівень хибнопозитивних результатів, який спостерігається в статистиці держав-членів ЄС, може поставити під сумнів адекватність і пропорційність системи.¹⁴¹ Тому Суд ЄС підкреслив важливість регулярного перегляду суворой необхідності дотримання заздалегідь визначених критеріїв.¹⁴² Він також зазначив, що держави-члени ЄС повинні встановити чіткі та точні правила для скеровування процесу індивідуальної перевірки з метою запобігання як дискримінаційним результатам, так і помилковим збігам, які передаються відповідним органам, що може несправедливо піддати пасажирів підозрі в причетності до тероризму або тяжких злочинів. Крім того, як зазначалося вище, Суд також зазначив, що висновки, зроблені на основі індивідуальних перевірок людьми, повинні мати перевагу над висновками, зробленими автоматизованими системами.¹⁴³
86. Розробникам відповідних нормативно-правових актів слід запровадити ефективні гарантії дотримання прав людини для захисту пасажирів від неправомірної підозри у причетності до тероризму чи інших тяжких злочинів та утримуватися від дискримінаційного профілювання на основі даних PNR. У переліку завдань Національного контактного пункту у статті 15 Законопроекту згадується «моніторинг, обробка та аналіз даних запису реєстрації пасажирів [...] з метою оновлення, актуалізації, створення (скасування) профілів ризику або критеріїв ідентифікації осіб, які можуть бути причетними до терористичної діяльності». Важливо, щоб ці критерії та профілі були цільовими, пропорційними та конкретними, і щоби проєкт Закону відображав ці вимоги. Проєкт Закону повинен зобов'язати відповідні органи надавати необхідні настанови для проведення індивідуальних перевірок з метою запобігання дискримінаційним результатам. Ці критерії повинні регулярно переглядатися і за жодних обставин не повинні ґрунтуватися на «расовій» чи етнічній належності особи, її політичних поглядах, релігійних чи філософських переконаннях, членстві

138 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року. У п. 103 Суд ЄС зазначає, посилаючись на попередню практику, що «на цьому тлі слід мати на увазі, що Суд вже постановляв, що ступінь втручання, яке тягне за собою автоматизований аналіз даних PNR щодо прав, закріплених у статтях 7 і 8 Хартії, по суті, залежить від заздалегідь визначених моделей і критеріїв, а також від баз даних, на яких ґрунтується цей тип обробки даних (Висновок 1/15 (Угода між ЄС і Канадою про PNR) від 26 липня 2017 року, EU:C:2017:592, п. 172)».

139 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 197.

140 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 198.

141 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 123.

142 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 201.

143 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 205-208.

- у профспілці, стані здоров'я, сексуальному житті чи сексуальній орієнтації.¹⁴⁴ У статті 15 проекту Закону слід зробити пряме посилання на це. Аналогічний підхід слід застосовувати до баз даних та контрольних списків з метою забезпечення прозорості критеріїв для включення до них та забезпечення виправлення у разі неправомірного включення. Критерії включення осіб до таких списків мають бути чітко сформульовані на основі вузького і точного визначення терористичних злочинів і тяжких злочинів. Крім того, для захисту від свавілля мають бути передбачені суворі процесуальні гарантії, зокрема, ефективні засоби правового захисту для оскарження неправомірного включення до списку, а також ефективні заходи для забезпечення виключення зі списку на практиці, в тому числі у випадках, коли контрольні списки або дані передаються на транснаціональному рівні.
87. Проекту Закону також бракує чіткого положення про захист від непрямої дискримінації під час аналізу даних. Профілювання на основі корельованих атрибутів, як-от історія подорожей, громадянство чи інші ознаки, може ненавмисно призвести до упереджених результатів, які матимуть непропорційний вплив на певні групи. Це загрожує порушенням принципів рівності та права на недискримінацію, передбачених статтею 26 МПГПП, статтею 14 ЄКПЛ та Протоколом № 12 до ЄКПЛ, а також статтею 21 Хартії основних прав ЄС. У зв'язку з цим, до проекту Закону слід включити пряме посилання на заборону непрямої дискримінації під час і в результаті обробки даних.
88. Загалом, настійною рекомендацією для компетентних органів є забезпечити, щоби співробітники, які обробляють дані API/PNR, проходили належну підготовку з прав людини та були обізнані з потенційними наслідками для прав людини, пов'язаними з цими системами.
89. Нарешті, стаття 16 містить перелік завдань Національної системи обробки PNR. У пункті 4 наведено загальне положення про недискримінацію. Вітаючи такий підхід, автори вважають, що положення про недискримінацію можна було би доповнити посиланням на членство в профспілці та стан здоров'я пасажирів, як це має місце в стандартах ІКАО та Директиви ЄС про PNR.¹⁴⁵

РЕКОМЕНДАЦІЯ F.

Запровадити ефективні гарантії дотримання прав людини для захисту пасажирів від неправомірної підозри у причетності до тероризму або інших тяжких злочинів та утриматися від дискримінаційного профілювання на основі даних PNR у переліку завдань Національного контактного пункту, наведеному в статті 15. Критерії ризику та профілі повинні бути цільовими, пропорційними та конкретними, а також зобов'язувати відповідні органи надавати необхідні настанови для проведення індивідуальних перевірок з метою запобігання дискримінаційним результатам.

5. ОБОВ'ЯЗОК ІНФОРМУВАТИ ТА БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ

90. GDPR, Директива ЄС про PNR, модернізована Конвенція 108 (ще не ратифікована Україною) та інші відповідні інструменти закріплюють право на захист даних.

¹⁴⁴ Стаття 6 (4) Директиви ЄС про PNR.

¹⁴⁵ Преамбула Директиви ЄС про PNR, п. 15, Додаток 9 до ІКАО, стаття 9.30 b)

Одним з ключових прав є право бути поінформованим про обробку власних даних. Стаття 22 проєкту Закону покладає на авіаперевізників обов'язок інформувати пасажирів про обробку їхніх даних. Однак інформування пасажирів про обробку їхніх персональних даних та доступ до них також є обов'язком держави. Директива ЄС про PNR передбачає, що «держави-члени повинні забезпечувати надання пасажирам точної інформації, яка повинна бути легкодоступною та легкозрозумілою, стосовно збору даних PNR, їх передавання до PIU та їхніх прав як суб'єктів даних».¹⁴⁶ Тому рекомендовано, **щоби проєкт Закону передбачав підхід, згідно з яким пасажирів інформують про обробку їхніх персональних даних чіткою та простою мовою, яку вони розуміють.**

91. Центральним положенням проєкту Закону є стаття 22, яка стосується захисту персональних даних. Вона передбачає, що облік операцій з обробки (збір, зберігання, перегляд, розкриття та видалення) забезпечується Національним центром (для даних API) та Національним контактним пунктом (для даних PNR). Положення покладає на Національний центр та Національний контактний пункт відповідальність за «безпеку» персональних даних. У разі порушення ці органи зобов'язані інформувати Уповноваженого Верховної Ради України з прав людини та суб'єкта персональних даних. Це відповідає міжнародним та європейським стандартам, зокрема статті 13 (8) Директиви ЄС про PNR.
92. Однак, за стандартами ІКАО, держави мають додаткові зобов'язання щодо захисту персональних даних, особливо щодо прав суб'єктів даних. У зв'язку з цим, стаття 8 модернізованої Конвенції РЄ 108 передбачає чіткі зобов'язання органів державної влади відповідати на запити щодо існування персональних даних, повідомляти ці дані суб'єкту даних, виправляти або видаляти дані у разі незаконного збору/обробки,¹⁴⁷ хоча існують винятки в інтересах «захисту державної безпеки». Ці стандарти визнаються не лише Конвенцією Ради Європи, але й міжнародними інструментами «м'якого права», як-от [*Керівні принципи ООН щодо регламентації комп'ютеризованих картотек, що місять персональні дані*](#) 1988 року (Принцип 4) та [*Принципи Тиване*](#) (Частина III).¹⁴⁸ Якщо ці питання вже достатньою мірою не врегульовані в Законі України «Про захист персональних даних», **проєкт Закону**

146 Преамбула Директиви ЄС про PNR, п. 29. Наприклад, уряд **Нідерландів** має спеціальну веб-сторінку, на якій простою, нетехнічною мовою подано огляд того, як дані про пасажирів збираються/використовуються різними державними установами, а також огляд аспектів захисту даних. На ній також міститься інформація для пасажирів, які бажають отримати доступ до цих даних, а також інформація про те, як їх можна оскаржити/видалити (див. Уряд Нідерландів, Інформація для пасажирів авіаперевезень.

<https://www.government.nl/topics/aviation/air-passenger-travel-information>). У **Канаді** обробка даних API/PNR регулюється Законом про митницю, Законом про захист приватного життя, Положенням про інформацію про пасажирів та іншими нормативно-правовими актами. Основним національним органом, що збирає дані API/PNR, є Агентство прикордонної служби Канади (CBSA). Агентство опублікувало Настанови щодо доступу, використання та розкриття даних API та PNR, а також інформації перед вильотом, які демонструють належну практику, особливо щодо доступу суб'єктів даних до своїх персональних даних; див. Уряд Канади, [Guidelines](#) for the access to, use, and disclosure of advance passenger information (API), passenger name record (PNR) data and pre-departure air exit information, пп. 42-43.

147 Стаття 8 модернізованої Конвенції РЄ № 108 зазначає, що "Будь-яка особа має право: а) встановлювати існування файлу персональних даних для автоматизованої обробки, його головні цілі, а також особу та постійне місце проживання чи головне місце роботи контролера файлу; б) отримувати через розумні проміжки часу та без надмірної затримки або витрат підтвердження або спростування факту зберігання персональних даних, що її стосуються, у файлі даних для автоматизованої обробки, а також отримувати такі дані у доступній для розуміння формі; с) вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися всупереч положенням внутрішнього законодавства, що запроваджують основоположні принципи, визначені у статтях 5 і 6 цієї Конвенції; д) використовувати засоби правового захисту у разі невиконання передбаченого у пунктах б і с цієї статті прохання про підтвердження або у відповідних випадках про надання, виправлення або знищення персональних даних».

148 Див. також Спеціальний комітет ПА ОБСЄ з протидії тероризму «Зміцнення безпеки кордонів та обміну інформацією в регіоні ОБСЄ – Анкета щодо парламентського нагляду», с. 13. Наприклад, у **Німеччині** обробка даних API передбачена законодавчими положеннями, що містяться у Федеральному законі про поліцію. Запити на отримання даних реєструються, а обробка даних API підлягає постійному аудиту та нагляду з боку спеціалістів. Закон також передбачає суворі правила щодо захисту персональних даних (наприклад, щодо залучення Федерального уповноваженого з питань захисту даних та свободи інформації, знеособлення даних пасажирів разом із реєстрацією даних), яких необхідно дотримуватися під час обробки даних пасажирів.

можна було би суттєво посилити шляхом чіткого відображення в ньому таких прав на захист даних.

93. Позитивним є те, що стаття 21 проекту Закону передбачає призначення співробітників з питань захисту даних PNR. Однак це положення слід посилити та привести у відповідність до вищезазначених стандартів. По-перше, відповідно до Директиви ЄС про PNR, співробітники з питань захисту даних мають бути забезпечені засобами для ефективного та незалежного виконання своїх обов'язків і завдань.¹⁴⁹ **Рекомендовано включити аналогічне положення до проекту Закону, щоби забезпечити ефективну й незалежну роботу співробітників з питань захисту даних.** По-друге, Директива ЄС про PNR вимагає від держав забезпечити, «*право суб'єкта даних контактувати зі старшим спеціалістом з питань захисту даних через єдиний контактний пункт щодо будь-яких питань, пов'язаних з опрацюванням даних PNR такого суб'єкта даних*».¹⁵⁰ **За відсутності такого положення в проекті Закону слід передбачити засоби, за допомогою яких суб'єкти даних можуть безпосередньо зв'язатися зі співробітниками з питань захисту даних.**
94. При тому, що в статті 21 проекту Закону зазначається, що співробітники з питань захисту даних мають доступ до всіх даних, які опрацьовуються в системі накопичення даних запису реєстрації пасажирів Національної системи обробки PNR, слід нагадати, що Суд ЄС у своєму рішенні уточнив: «хоча співробітник з питань захисту даних має доступ до всіх даних, які обробляє підрозділ з питань інформації про пасажирів (PIU), цей доступ повинен обов'язково охоплювати заздалегідь визначені критерії та бази даних, використовувані цим підрозділом, з метою гарантувати ефективність і високий рівень захисту даних, що їх цей співробітник повинен забезпечити відповідно до пункту 37 цієї Директиви».¹⁵¹
95. В останньому абзаці статті 21 проекту Закону зазначено, що співробітники з питань захисту даних PNR «взаємодіють» з Уповноваженим Верховної Ради України з прав людини. Однак незрозуміло, що мається на увазі під словом «взаємодіють». **Слід роз'яснити, що співробітники з питань захисту даних PNR можуть безпосередньо та конфіденційно повідомляти про порушення Уповноваженому, а також можуть передавати справи на розгляд Уповноваженого та здійснювати інші дії.**

РЕКОМЕНДАЦІЯ G.

Роз'яснити у статті 21 проекту Закону, що співробітники з питань захисту даних PNR можуть безпосередньо та конфіденційно повідомляти про порушення Уповноваженому Верховної Ради України з прав людини, а також можуть передавати справи на розгляд Уповноваженого та вживати інших заходів.

¹⁴⁹ Стаття 5 (2) Директиви ЄС про PNR.

¹⁵⁰ Стаття 5 (3) Директиви ЄС про PNR.

¹⁵¹ Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 212.

6. НЕЗАЛЕЖНИЙ НАГЛЯД

96. Відповідно до стандартів ІКАО, держави повинні призначити один або декілька компетентних національних органів, уповноважених здійснювати незалежний нагляд за захистом даних PNR та визначати, чи дані PNR збираються, використовуються, обробляються та захищаються з повним дотриманням прав і свобод людини.¹⁵² Так само, згідно з Директивою ЄС про PNR, держави-члени ЄС повинні створити «Національний наглядовий орган» з метою захисту основних прав у зв'язку з обробкою персональних даних (див. також статті 51-59 GDPR та статтю 15 Модернізованої конвенції 108). Такий орган повинен бути структурно й операційно незалежним відповідно до статей 51 та 52 GDPR, опрацьовувати скарги, подані будь-яким суб'єктом даних, розслідувати випадки й інформувати суб'єктів даних про стан і результати розгляду їхніх скарг упродовж обґрунтованого строку, а також підтверджувати законність опрацювання даних, проводити розслідування, інспектування і аудити відповідно до національного права з власної ініціативи або на підставі скарг. Будь-який суб'єкт даних також повинен бути поінформований про здійснення своїх прав.¹⁵³
97. Стаття 23 проєкту Закону визначає Уповноваженого Верховної Ради України з прав людини як наглядовий орган. Однак важливо, щоби на додачу до положень проєкту закону Уповноваженому було надано правовий мандат, достатні технічні, людські та фінансові ресурси і повноваження для ефективного здійснення нагляду за діяльністю Національного центру та Національного контактного пункту, як це передбачено Директивою про PNR. **Рекомендовано інтегрувати ці аспекти до закону, що регулює діяльність Уповноваженого Верховної Ради України з прав людини, та зробити відповідне посилання у проєкті Закону.** Крім того, оскільки у статті 23 проєкту Закону йдеться про *парламентський* контроль за відповідністю його положень законодавству про захист даних, виникає запитання, чи діє Уповноважений з прав людини як незалежний наглядовий орган у сенсі статті 52 GDPR. Остання передбачає, серед іншого, що «кожен наглядовий орган діє абсолютно незалежно під час виконання своїх завдань та здійснення своїх повноважень згідно з цим Регламентом» і що «член або члени кожного наглядового органу, під час виконання своїх завдань та здійснення своїх повноважень згідно з цим Регламентом, повинні залишатися вільними від зовнішнього впливу, прямого чи опосередкованого, та не повинні запитувати чи приймати вказівки від будь-якої особи...». Тому слід забезпечити, щоби будь-який нагляд за дотриманням законодавства про захист персональних даних незалежно здійснювався уповноваженим органом, якому надано необхідні ресурси та повноваження для виконання його функцій у спосіб, що відповідає міжнародним документам.
98. Нарешті, стаття 77 GDPR передбачає, що кожен суб'єкт даних має право подати скаргу до наглядового органу. Такий захист не передбачений у проєкті Закону. **Рекомендовано чітко передбачити цей механізм подання скарг у проєкті Закону та відобразити його в законі, що регулює діяльність Уповноваженого Верховної Ради України з прав людини.**
99. У зв'язку з цим варто зазначити, що Суд ЄС у справі *Ligue des droits humains ASBL* постановив, що відповідно до Директиви ЄС про PNR національний наглядовий орган забезпечує моніторинг законності автоматизованої обробки, здійснюваної PIU у зв'язку з попередньою оцінкою. Цей моніторинг охоплює, серед іншого,

152 Додаток 9 до Конвенції ІКАО, стаття 9.29.

153 Стаття 15 Директиви ЄС про PNR.

перевірку того, чи не є ці операції дискримінаційними. При тому, що положення стосовно співробітників з питань захисту даних передбачають, що вони мають доступ до всіх даних, які обробляються PIU, і що такий доступ повинен обов'язково охоплювати заздалегідь визначені критерії та бази даних, використовувані цим підрозділом, розслідування, перевірки та аудити, які проводить національний наглядовий орган згідно з відповідними положеннями Директиви ЄС про PNR, також можуть стосуватися цих заздалегідь визначених критеріїв та баз даних, аби гарантувати ефективність і високий рівень захисту даних, який ці співробітники повинні забезпечити.¹⁵⁴ **Відповідно, Уповноважений з прав людини, для належного здійснення своїх повноважень, повинен мати повний і безперешкодний доступ до всієї інформації, що обробляється Національним контактним пунктом (PIU), а також до заздалегідь визначених критеріїв і баз даних.**

РЕКОМЕНДАЦІЯ Н.

Забезпечити, щоби будь-який нагляд за дотриманням законодавства про захист даних незалежно здійснювався уповноваженим органом, якому надано необхідні ресурси та повноваження для виконання свого мандату у спосіб, що відповідає міжнародним документам, а також забезпечити, щоби цей орган або **Уповноважений Верховної Ради України з прав людини мав повний і безперешкодний доступ до всієї інформації, що обробляється Національним контактним пунктом, а також до заздалегідь визначених критеріїв і баз даних, необхідних для виконання свого мандату.**

7. МЕХАНІЗМИ ОСКАРЖЕННЯ ТА СУДОВОГО КОНТРОЛЮ

100. Окрім права подавати скарги до наглядового органу, особи мають право на ефективний судовий захист, що дозволяє їм звертатися до суду щодо потенційних порушень захисту даних. Право на судовий захист визнається як статтею 47 Хартії основних прав ЄС, так і статтею 13 ЄКПЛ. Стаття 78 GDPR передбачає право на дієвий засіб правового захисту проти наглядового органу. Такий засіб правового захисту, зокрема, гарантує право на судовий перегляд рішень органів захисту даних. Стандарт 9.26 Додатку 9 до Чиказької конвенції закликає держави передбачити адміністративні та судові механізми правового захисту, що дозволяли б особам звертатися по правовий захист від незаконної обробки даних PNR органами державної влади, а також передбачити відповідні механізми, встановлені їхньою правовою та адміністративною системою, щоб особи могли отримати доступ до своїх даних PNR та вимагати, за необхідності, виправлення, видалення чи внесення приміток.¹⁵⁵
101. Стаття 26 проєкту Закону передбачає, що дії або рішення Національного центру, Національного контактного центру або уповноважених органів можуть бути оскаржені в судовому порядку, хоча немає жодних посилань на конкретний

154 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 212.

155 Конвенція ІКАО, Додаток 9, стандарт 9.26.

компетентний суд (суди) або відповідну процедуру. До цього положення можна було би включити перехресне посилання на застосовне законодавство та процедуру, хіба що вони достатньою мірою описані в Законі України «Про захист персональних даних»; тоді до цього положення варто було би включити відповідне посилання.

102. Для того, щоби право на судовий захист було ефективним на практиці, суб'єктам даних повинна бути надана вичерпна інформація зрозумілою їм мовою, щоб вони могли оскаржити законність автоматизованої обробки та подальшого індивідуального перегляду. Аналогічно, в контексті правових засобів захисту, вичерпна інформація повинна бути надана суду та зацікавленим особам для аналізу законності рішення, ухваленого компетентними органами, тобто підстав та доказів.¹⁵⁶ В обох ситуаціях можуть застосовуватися певні винятки щодо надання інформації.¹⁵⁷ Проєкт Закону слід доповнити відповідним положенням.

8. РЕКОМЕНДАЦІЇ ЩОДО ПРОЦЕСУ ПІДГОТОВКИ Й УХВАЛЕННЯ ПРОЄКТУ ЗАКОНУ

103. Держави-учасниці ОБСЄ зобов'язалися забезпечити ситуацію, за якої «закони, ухвалені по завершенню відповідної публічної процедури, й адміністративні положення публікуються, що є умовою їх застосування» (Копенгагенський документ 1990 року, п. 5.8).¹⁵⁸ Крім того, ключові зобов'язання передбачають, що «законодавство буде розроблятися й ухвалюватися в результаті відкритого процесу, що відображає волю народу чи то безпосередньо, чи то через обраних ним представників» (Московський документ 1991 року, п. 18.1).¹⁵⁹ БДПЛ у [Керівництві з демократичного законотворення для вдосконалення законодавства](#) (2024) підкреслює важливість заснованого на фактах, відкритого, прозорого, партисипативного й інклюзивного законотворчого процесу, який надає реальні можливості всім зацікавленим сторонам робити свій внесок протягом усього законотворчого процесу.¹⁶⁰
104. Зрозуміло, що у процесі розробки проєкту Закону Служба безпеки України прагнула провести консультації з різними зацікавленими сторонами, включаючи інші установи сектору безпеки й оборони та міжнародних партнерів. Це загалом позитивний підхід, який в цілому відповідає зобов'язанням в рамках ОБСЄ.
105. Публічні консультації є засобом відкритого і демократичного врядування, оскільки вони сприяють підвищенню прозорості та підзвітності державних інституцій і допомагають виявити потенційні суперечності ще до ухвалення закону.¹⁶¹ Для того, щоби консультації стосовно законопроектів і політик були ефективними, вони мають бути інклюзивними і надавати відповідним зацікавленим сторонам достатньо часу для підготовки та подання рекомендацій щодо законопроектів.

156 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, пп. 2009-211. Див. також ЄРЗД, [Заява 2/2025 Європейської ради із захисту даних щодо імплементації Директиви про PNR у світлі рішення Суду ЄС C-817/19](#), ухвалена 13 березня 2025 року, п. 19.

157 Суд ЄС, [C-817/19](#) [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Законність записів реєстрації пасажирів у ЄС), 21 червня 2022 року, п. 210.

158 Доступно за посиланням <<http://www.osce.org/fr/odihr/elections/14304>><http://www.osce.org/fr/odihr/elections/14304>.

159 Доступно за посиланням <<http://www.osce.org/fr/odihr/elections/14310>><http://www.osce.org/fr/odihr/elections/14310>.

160 БДПЛ, Керівництво з демократичного законотворення для вдосконалення законодавства (січень 2024 року), зокрема Принципи 5, 6, 7 і 12. Див. також Венеційська комісія, [Мірило правовладдя \(Контрольний список запитань для оцінки дотримання верховенства права\)](#), CDL-AD(2016)007, частина II.A.5.

161 Рекомендації щодо сприяння більш ефективній участі об'єднань громадян у процесах прийняття державних рішень (від учасників Форуму громадянського суспільства для презентації на додатковій нараді ОБСЄ з питань людського виміру), Відень, 15-16 квітня 2015 року.

Держава також повинна забезпечити достатній і своєчасний механізм зворотного зв'язку, за допомогою якого органи державної влади повинні визнавати внесок учасників консультацій і реагувати на подані пропозиції.¹⁶² Щоби гарантувати ефективну участь, механізми консультацій повинні дозволяти робити внесок на ранній стадії, починаючи з відправного етапу розробки політики *і протягом усього процесу*,¹⁶³ що охоплює не лише підготовку законопроєкту, а і його обговорення в парламенті, чи то під час громадських слухань, чи то під час засідань парламентських комітетів. Враховуючи чутливість і значущість такої широкомасштабної реформи, дуже важливо почути всі голоси, навіть ті, які можуть бути критично налаштовані щодо запропонованих ініціатив, з метою вирішення порушених питань і досягнення широкого політичного консенсусу та громадської підтримки такої реформи у країні. Зрештою, це, як правило, покращує імплементацію законів після їх ухвалення та підвищує довіру громадськості до державних інституцій загалом.

106. Розробники проєкту Закону підготували Пояснювальну записку до нього, в якій надається обґрунтування необхідності запропонованої реформи, але не згадується про дослідження й оцінку впливу, на яких базуються ці висновки. В принципі, закони та державні рішення повинні готуватися, обговорюватися й ухвалюватися на основі добре викладених аргументів, наукових доказів і даних, зокрема інформації, отриманої в результаті оцінки впливу та консультацій з громадськістю й іншими зацікавленими сторонами.¹⁶⁴ З огляду на потенційний вплив проєкту Закону на реалізацію прав людини та основних свобод, важливо провести поглиблену оцінку регуляторного впливу (див. також статтю 35 GDPR), в тому числі на дотримання прав людини, яка повинна містити належний аналіз проблеми з використанням науково обґрунтованих методів для визначення найбільш ефективного та дієвого варіанту регулювання.¹⁶⁵ Якщо такої оцінки впливу проведено ще не було, розробникам слід провести такий поглиблений аналіз, виявити наявні проблеми та відповідно адаптувати запропоновані рішення.
107. У світлі вищезазначеного, **органам державної влади рекомендовано забезпечити проведення інклюзивних, широких і ефективних консультацій щодо проєкту Закону, в тому числі з організаціями громадянського суспільства, авіакомпаніями, а також забезпечити рівні можливості для участі жінок і чоловіків. Відповідно до вищезазначених принципів, такі консультації мають відбуватися своєчасно, на всіх етапах законотворчого процесу, в тому числі в парламенті. Важливим елементом належної законотворчості є також запровадження послідовної системи моніторингу й оцінки імплементації законодавства, яка б ефективно відстежувала функціонування й ефективність проєкту Закону після його ухвалення.**¹⁶⁶

[КІНЕЦЬ ТЕКСТУ].

162 БДПЛ, Керівництво з демократичного законотворення для вдосконалення законодавства (2024), Принцип 7.

163 БДПЛ, Керівництво з демократичного законотворення для вдосконалення законодавства (2024), Принцип 7.

164 Керівництво з демократичного законотворення для вдосконалення законодавства (січень 2024 року), Принцип 5, Законотворення на основі фактичних даних.

165 Див., наприклад, БДПЛ, Попередня оцінка законодавчого процесу в Республіці Узбекистан (11 грудня 2019 року), Рекомендації L і M; та Венеційська комісія, Мірило правовладдя (Контрольний список запитань для оцінки дотримання верховенства права), CDL-AD(2016)007, частина II.A.5.

166 БДПЛ, Керівництво з демократичного законотворення для вдосконалення законодавства (січень 2024 року), п. 23. Наприклад, ОЕСР, Передові регуляторні практики в Європейському Союзі, розділ 4: Ex post огляд законів і нормативних актів Європейського Союзу (2010).