

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ



2025

Пам'ятка

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Пам'ятка щодо особливостей захисту персональних даних в діяльності Національної поліції України підготовлена за результатами трьох раундів практичних консультацій з представниками Департаменту головної інспекції та дотримання прав людини Національної поліції України, що відбувались з квітня по червень 2025 року. Пам'ятка містить загальний огляд питань щодо обробки та захисту персональних даних у діяльності Національної поліції України та надає практичні поради щодо їх застосування. Брошура присвячена практичним аспектам діяльності представників Національної поліції, що пов'язана зі збором та обробкою персональних даних, документальним забезпеченням та аналітичною роботою у контексті національного та міжнародного регулювання, принципів та стандартів Ради Європи та Європейського Союзу у цій сфері.

© Shutterstock, фото на обкладинці

Погляди, викладені в цьому документі, є відповідальністю його авторів і можуть не співпадати з офіційною політикою Ради Європи.

ЗМІСТ

Вступ	5
1. Національне законодавство в галузі захисту персональних даних.	7
2. Міжнародні зобов'язання України в галузі захисту персональних даних.	8
3. Поняття «Персональні дані»	9
4. Спеціальні категорії персональних даних (чутливі персональні дані)	10
5. Обробка персональних даних	11
6. Суб'єкти відносин, пов'язані з персональними даними	12
7. Володільці та розпорядники: ролі та відповідальність	13
8. Принципи обробки персональних даних	14
9. Законність обробки персональних даних.	16
10. Строки зберігання персональних даних	17
11. Підстави обробки персональних даних	18
12. Правові підстави для обробки персональних даних у діяльності Національної поліції України.	19
13. Неможливість використання згоди співробітниками Національної поліції України як правової підстави для обробки персональних даних ...	20
14. Права суб'єкта персональних даних	22
15. Обмеження реалізації прав суб'єктів персональних даних.	24
16. Надання доступу іншим суб'єктам відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи або групи осіб.	25
17. Оплата за послуги з надання доступу до персональних даних	26
18. Підстави видалення з державних баз даних та реєстрів відомостей про суб'єкта за його зверненням	27
19. Порядок організації процесу обробки персональних даних	29
20. Внутрішні документи володільця	31
21. Реєстр операцій з обробки даних	33
22. Обов'язки щодо захисту персональних даних для посадових осіб володільців і розпорядників даних	34
23. Технічні та організаційні заходи, впроваджені в підрозділах Національної поліції України щодо належного захисту персональних даних	35
24. Уповноважений структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних під час їх обробки.	37

25. Система повідомлення про порушення безпеки персональних даних	38
26. Захист даних за призначенням та захист даних за замовчуванням	40
27. Оцінка впливу на захист даних	41
28. Контроль за дотриманням законодавства про захист персональних даних	42
29. Перевірки як форма контролю за дотриманням законодавства про захист персональних даних	44
30. Департамент моніторингу дотримання інформаційних прав Секретаріату Уповноваженого Верховної Ради України з прав людини	46
31. Підвищення обізнаності громадськості, представників органів державної влади та бізнесу в галузі захисту персональних даних	48
32. Відповідальність і санкції	49
33. Порядок дій співробітника Національної поліції України у разі, якщо під час затримання або складання адміністративного протоколу особа відмовляється надавати персональні дані	50
34. Захист персональних даних осіб у кримінальному провадженні	51
35. Транскордонне передання персональних даних	53
36. Європол	54
37. Співробітництво між Україною Європолом	55
38. Директива (ЄС) 2016/680	56
39. Відеомоніторинг стану публічної безпеки за допомогою систем розпізнавання обличчя	57
40. Як забезпечити конфіденційність даних під час відеофіксації?	59
41. Чи має право поліцейський вести фото-, відеофіксацію документів або обличчя особи на місці події?	61
42. Які вимоги існують щодо використання мобільних застосунків (вайберу, вацапу) для обміну службовою інформацією?	63
43. Ключові правові позиції Верховного Суду в справах, що стосуються принципів і підстав обробки персональних даних	65
44. Реформа захисту персональних даних в Україні	66
45–50. Приклади кейсів щодо доступу до персональних даних третіх осіб	68
Використані джерела	79
Summary	81

ВСТУП

Дотримання найвищих стандартів захисту персональних даних у правоохоронній галузі має першочергове значення для забезпечення безпеки і захисту прав кожного громадянина, зокрема права на приватність.

Технологія та обробка персональних даних — незамінний інструмент для поліції в боротьбі зі злочинністю. У цьому контексті чіткі та послідовні правила щодо захисту даних для Національної поліції України мають стати фундаментальною основою для гарантування безпеки і захисту прав кожного громадянина та поліпшення співпраці між правоохоронними органами.

Ідеєю для розроблення Пам'ятки щодо особливостей захисту персональних даних в діяльності Національної поліції України стали три раунди практичних консультацій з представниками Департаменту головної інспекції та дотримання прав людини Національної поліції України, які відбувалися з квітня по червень 2025 року.

Мета розроблення Пам'ятки — підготування роз'яснень і практичних рекомендацій щодо застосування національного законодавства у сфері захисту персональних даних у діяльності Національної поліції України.

Пам'ятка охоплює такі питання:

- національне законодавство в галузі захисту персональних даних;
- термінологію в галузі захисту персональних даних;
- реалізацію принципів обробки персональних даних;
- підстави для обробки персональних даних;
- вимоги до обробки спеціальних категорій персональних даних;
- права суб'єктів персональних даних;
- обов'язки володільця і розпорядника персональних даних;
- технічні та організаційні заходи захисту персональних даних;

- порядок призначення, функціональні обов'язки та вимоги до відповідальної особи з питань захисту персональних даних;
- врегулювання передання персональних даних на територію іноземних держав та міжнародних організацій;
- відповідальність та санкції за порушення положень законодавства в галузі захисту персональних даних;
- практичні питання щодо обробки та захисту персональних даних в діяльності співробітників Національної поліції України.

Пам'ятка має стати практичним інструментом для співробітників Національної поліції України в питанні захисту персональних даних у розв'язанні поставлених перед ними робочих завдань.

Автори: **Олександр Шевчук, Лілія Олексюк**, національні консультанти Ради Європи із захисту персональних даних

1. НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО В ГАЛУЗІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

- Конституція України, зокрема, стаття 32;
- Закон України «Про захист персональних даних»;
- Типовий порядок обробки персональних даних;
- Порядок здійснення Уповноваженим ВРУ з прав людини контролю за додержанням законодавства про захист персональних даних;
- Порядок повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних у разі їх обробки, а також оприлюднення вказаної інформації;
- КУпАП: ст. 188–39 «Порушення законодавства у галузі захисту персональних даних», ст. 188–40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»;
- Кримінальний кодекс України: ст. 182 «Порушення недоторканності приватного життя».

2. МІЖНАРОДНІ ЗОБОВ'ЯЗАННЯ УКРАЇНИ В ГАЛУЗІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Україна — сторона Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108). У травні 2018 року Рада Європи ухвалила Протокол CETS № 223, яким внесено зміни до Конвенції 108. Конвенція 108+ враховує більшість викликів, спричинених розвитком інформаційних і комунікаційних технологій та посилює вимоги щодо її імплементації. Отже, перед Україною постало питання ратифікації вказаного Протоколу, та увідповіднення законодавства до вимог оновленої Конвенції 108+.

Угода про асоціацію між Україною та Європейським Союзом вимагає увідповіднення законодавства України до європейських стандартів, що стосується галузі захисту персональних даних. Серед іншого, стаття 15 Угоди про асоціацію передбачає, що Україна та ЄС домовилися про співробітництво з метою забезпечення належного рівня захисту персональних даних відповідно до європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи.

Дорожня карта з питань верховенства права, яку затвердив Кабінет Міністрів України 14 травня 2025 року, передбачає увідповіднення національного законодавства в галузі захисту персональних даних до Конвенції 108+, Регламенту (ЄС) 2016/679 та Директиви (ЄС) 2016/680.

3. ПОНЯТТЯ «ПЕРСОНАЛЬНІ ДАНІ»

Персональні дані — це інформація про особу (суб'єкта даних), за допомогою якої її можна прямо чи опосередковано ідентифікувати. Важливо підкреслити, що персональні дані — це лише дані про особу. Дані про компанію або установу не вважаються персональними.

Ідентифікованою вважається особа, яку можна безпомилково вирізнити серед інших осіб. Зазвичай для ідентифікації достатньо знати ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу, або цифровий номер, присвоєний особі (наприклад, ідентифікаційний номер). Водночас не завжди потрібен повний набір таких відомостей. Деколи достатньо меншої кількості даних, щоб ідентифікувати особу. Наприклад, фотографія чи відеозапис можуть бути достатніми для того, щоб встановити конкретну особу.

***Приклад.** Розглянемо базу даних «Розшук» Національної поліції України. Це автоматизований банк відомостей, у якому обробляється інформація щодо розшуку осіб. Для розшуку осіб Національна поліція України збирає інформацію про прізвище, власне ім'я та по батькові; фотографію; дату народження; опис зовнішності; особливі прикмети; стать; місце виявлення; опис одягу; зріст; вік.*

Отже, набір даних, достатній для ідентифікації особи, залежить від контексту та особливостей конкретної операції з обробки персональних даних.

4. СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ (ЧУТЛИВІ ПЕРСОНАЛЬНІ ДАНІ)

Важливий у контексті діяльності Національної поліції України, є характер даних про особу. Персональні дані поділяються на звичайні та спеціальні категорії персональних даних.

Спеціальні категорії персональних даних — це дані, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання чи членство в профспілках, генетичні дані, біометричні дані, що використовуються для однозначної ідентифікації особи, дані про здоров'я, а також дані про статеве життя та сексуальну орієнтацію.

Вказані категорії персональних даних характеризуються як чутливі персональні дані, бо розкривають відомості чутливого характеру щодо особи або їх неконтрольоване використання може стати причиною дискримінації відповідного суб'єкта даних.

***Приклад.** Національна поліція України збирає біометричні дані особи, зокрема шляхом дактилоскопіювання, у випадках, передбачених Кримінальним процесуальним кодексом України.*

5. ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ

Обробка персональних даних — це будь-яка операція, що виконується з даними: збір, організація, зберігання, зміна, ознайомлення, використання, передання, комбінування, видалення тощо.

***Приклад.** Національна поліція України виконує операції з обробки персональних даних під час проведення негласних слідчих (розшукових) дій та оперативно-розшукових заходів, ведення реєстрів та баз персональних даних.*

Варто пам'ятати, що неможливо скласти вичерпний перелік усіх операцій, які становлять обробку персональних даних, адже способи їх використання постійно змінюються з розвитком технологій. Раніше персональні дані зазвичай збирали безпосередньо від особи, наприклад, коли вона заповнювала анкету чи заяву. Сьогодні все частіше дані отримуються опосередковано через інтернет, мобільні додатки або «розумні» пристрої, що відстежують дії користувачів. Алгоритми можуть аналізувати таку інформацію, а саме: поведінку в мережі, місцеперебування, покупки чи активність у соціальних медіа, щоб зробити висновки про особу, її інтереси, стан здоров'я чи навіть професійну придатність.

6. СУБ'ЄКТИ ВІДНОСИН, ПОВ'ЯЗАНІ З ПЕРСОНАЛЬНИМИ ДАНИМИ

Суб'єкти відносин, пов'язаних із персональними даними, такі:

- суб'єкт персональних даних — фізична особа, персональні дані якої обробляються;
- володілець персональних даних — фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних і процедури їх обробки, якщо інше не визначено законом;
- розпорядник персональних даних — фізична чи юридична особа, якій володілець персональних даних або закон надає право обробляти ці дані від імені володільця;
- третя особа — будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володілець або розпорядник персональних даних передає персональні дані;
- Уповноважений Верховної Ради України з прав людини — посадова особа, що незалежно від інших державних органів та посадових осіб здійснює парламентський контроль за дотриманням конституційних прав і свобод людини і громадянина.

7. ВОЛОДІЛЬЦІ ТА РОЗПОРЯДНИКИ: РОЛІ ТА ВІДПОВІДАЛЬНІСТЬ

Національна поліція України є володільцем, коли вона визначає склад та зміст персональних даних і процедури обробки, необхідні для досягнення мети.

Національна поліція України обробляє персональні дані для своїх законних цілей, коли це необхідно для виконання покладених на неї завдань:

- забезпечення публічної безпеки і порядку;
- охорони прав і свобод людини, а також інтересів суспільства і держави;
- протидії злочинності;
- надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

Національна поліція України може бути розпорядником персональних даних.

***Наприклад**, статтею 25 Закону України «Про Національну поліцію» визначено, що поліція в рамках інформаційно-аналітичної діяльності формує та користується базами (банками) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України. Відповідно, в цьому разі володільцем буде Міністерство внутрішніх справ України, а розпорядником — Національна поліція України.*

Основна відмінність між володільцем і розпорядником полягає в тому, що розпорядник не може мати самостійної мети обробки, а обробляє персональні дані лише в межах мети, встановленої володільцем. Якщо розпорядник розпочне обробляти персональні дані з власною метою, в межах такої обробки він перетвориться на володільця.

8. ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Виконуючи будь-яку операцію з обробки персональних даних, співробітники Національної поліції України мають дотримуватися принципів обробки персональних даних.

Принцип перший — «законність, правомірність і прозорість». Персональні дані повинні оброблятися законним, правомірним і прозорим способом щодо суб'єкта даних. Будь-яка обробка персональних даних має бути законною та справедливою. До фізичної особи має бути прозоро донесено те, що її персональні дані збирають, використовують, переглядають або іншим чином обробляють.

Принцип другий — «конкретність цілей». Персональні дані можуть збиратися лише для конкретних, чітких і законних цілей і не повинні оброблятися в подальшому способом, несумісним із визначеними цілями.

Принцип третій — «мінімізація даних». Персональні дані повинні бути адекватними, відповідними та ненадмірними та обмежуватися тим, що необхідно для цілей, з якими вони обробляються.

Принцип четвертий — «точність». Персональні дані мають бути точними, вірогідними та оновлюватися, якщо це необхідно, для мети їх обробки. Необхідно вживати всіх раціональних заходів для того, щоб забезпечити точність персональних даних, які обробляються, а також усіх відповідних заходів для того, щоб неточні персональні дані були негайно видалені або виправлені.

Принцип п'ятий — «обмеження строків зберігання». Персональні дані не повинні зберігатися довше, ніж вони потрібні для цілей, для яких ці дані обробляються. Після того як мета була досягнута, персональні дані повинні бути знищені або знеособлені.

Принцип шостий — «цілісність та конфіденційність». Персональні дані повинні оброблятися так, щоб забезпечити їх ціліс-

ність і конфіденційність. Персональні дані повинні оброблятися так, щоб забезпечити належний рівень безпеки та конфіденційності цих персональних даних, зокрема для запобігання несанкціонованому доступові або несанкціонованому використанню персональних даних та обладнання, що застосовується для обробки.

Принцип сьомий — «підзвітність». Володілець несе відповідальність за дотримання принципів обробки персональних даних та має бути здатним це довести. Обов'язок доведення дотримання цих принципів покладається на володільця.

9. ЗАКОННІСТЬ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Щоб забезпечити законність обробки персональних даних, володільці та розпорядники повинні переконатися, що операція обробки виконується на законній підставі. Перш ніж ухвалити рішення щодо правової підстави для обробки персональних даних, володільці та розпорядники повинні розглянути такі елементи:

- **мета** операції з обробки персональних даних повинна бути чітко визначена перед вибором правової підстави для обробки;
- **пропорційність обробки:** якщо обробка персональних даних не необхідність (мета може бути належним обсягом досягнута без обробки), обробка персональних даних не може бути підкріплена жодною правовою підставою;
- **правова підстава** обробки повинна бути визначена до початку обробки персональних даних;
- **якщо мета обробки змінюється, але нова мета сумісна з початковою, можна продовжити процес обробки відповідно до первинної правової підстави.** Якщо нова мета не сумісна з початковою, обробку можна виконувати, якщо вона оснований на вимогах законодавства.

10. СТРОКИ ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ ДАНИХ

Строки зберігання персональних даних у Національній поліції України повинні визначатися з урахуванням:

- мети обробки персональних даних;
- категорій персональних даних, що обробляються;
- ступеня ризику порушення прав та свобод фізичних осіб унаслідок довготривалого зберігання їхніх персональних даних;
- положень законодавчих актів, якими визначено строк зберігання відповідних категорій персональних даних Національною поліцією України.

Персональні дані, строк зберігання яких закінчився, підлягають знищенню або знеособленню.

Видалення та знищення персональних даних робиться способом, що виключає подальшу можливість поновлення таких персональних даних.

Знеособлення робиться способом, що виключає можливість прямо чи опосередковано ідентифікувати особу.

Строки зберігання персональних даних, що обробляються в окремих реєстрах або інших інформаційних ресурсах, базах даних, які належать Національній поліції України, визначаються в окремих нормативно-правових актах Міністерства внутрішніх справ України або організаційно-розпорядчих актах Національної поліції України.

11. ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Основні вимоги щодо обробки персональних даних визначені Законом України «Про захист персональних даних».

Один із головних критеріїв законності обробки персональних даних — наявність правових підстав для такої обробки. **Підстави** — це певні передумови, у разі настання яких, можна обробляти персональні дані.

У статті 11 Закону України «Про захист персональних даних» закріплюється шість підстав для обробки персональних даних.

- згода особи на обробку її персональних даних;
- укладення та виконання правочину;
- життєво важливі інтереси суб'єкта даних;
- виконання володільцем персональних даних обов'язку, передбаченого законом;
- виконання офіційних повноважень органами державної влади та іншими суб'єктами владних повноважень;
- легітимні інтереси інших осіб.

Вказаний перелік підстав обробки персональних даних вичерпний.

12. ПРАВОВІ ПІДСТАВИ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Національна поліція України — це центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку.

Національна поліція України, як суб'єкт владних повноважень, зобов'язана діяти лише на підставі, в межах повноважень та способом, що передбачені Конституцією та законами України.

Правові підстави для обробки персональних даних співробітниками Національної поліції України:

- виконання повноважень, визначених законом, наприклад збирання доказів у розслідуванні злочинів;
- наявність юридичного зобов'язання, встановленого законом, наприклад виконання вимог Кодексу законів про працю України під час працевлаштування співробітників;
- укладання та виконання договору, наприклад закупівля товарів та послуг.

13. НЕМОЖЛИВІСТЬ ВИКОРИСТАННЯ ЗГОДИ СПІВРОБІТНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ЯК ПРАВОВОЇ ПІДСТАВИ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Відібрання згоди в суб'єкта персональних даних на обробку персональних даних органами державної влади за наявності інших підстав визначених законом — це порушення вимог Закону України «Про захист персональних даних».

Згода суб'єкта персональних даних — одна з шести підстав для обробки персональних даних. За наявності інших правових підстав, обробка персональних даних ведеться без згоди суб'єкта персональних даних.

Суттєва ознакою згоди на обробку персональних даних — добровільність (нема прямого або опосередкованого примусу під час її надання).

Суб'єкт персональних даних має право вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди; пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи вони невірні; заперечувати проти обробки своїх персональних даних. Якщо законом покладено обов'язок на певний орган державної влади обробляти персональні дані, то ані заперечення особи, ані відмова, ані застереження щодо обробки не можуть бути виконані.

Отже, якщо вимога обробки персональних даних для органу державної влади закріплена в законі, він не може вимагати від суб'єкта даних згоду. Бо в цьому разі особа буде позбавлена можливості відмовитися від обробки її персональних даних, а це, своєю чер-

гою, становить порушення принципу добровільності, обов'язкового елемента згоди.

Наприклад. Відповідно до законодавства кожен громадянин України, який досяг 14-річного віку, зобов'язаний отримати паспорт. Відповідно до статті 197 Кодексу про адміністративні правопорушення проживання громадян України без паспорта тягне за собою попередження. Органи державної влади не можуть використовувати згоду громадянина як підставу для збору його персональних даних у разі, коли така обробка обов'язкова за законом. У таких ситуаціях правовою підставою виступає норма закону, а не волевиявлення особи.

14. ПРАВА СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ

Суб'єкт персональних даних має такі права:

- знати про джерела збирання, мету їх обробки, місцеперебування або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, установлених законом;
- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;
- на доступ до своїх персональних даних;
- отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;
- пред'являти вмотивовану вимогу володільцеві персональних даних із запереченням проти обробки своїх персональних даних;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи вони невірні;
- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що невірні чи ганьблять честь, гідність і ділову репутацію фізичної особи;
- звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
- вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
- відкликати згоду на обробку персональних даних;
- знати механізм автоматичної обробки персональних даних;
- на захист від автоматизованого рішення, яке має для нього правові наслідки.

15. ОБМЕЖЕННЯ РЕАЛІЗАЦІЇ ПРАВ СУБ'ЄКТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Реалізація прав суб'єктів персональних даних, визначених Законом України «Про захист персональних даних», може бути обмежена. Будь-яке обмеження реалізації прав суб'єктів персональних даних повинно:

- 1) бути передбаченим законом;
- 2) вестися з метою недопущення:
 - розголошення службової інформації;
 - перешкоджання проведенню слідчих, розшукових, розвідувальних дій;
 - загроз для громадської чи національної безпеки;
 - загроз для життя, здоров'я чи порушення прав і свобод інших осіб.

Обсяг прав суб'єктів персональних даних стосовно окремих операцій з обробки їхніх персональних даних Національною поліцією України визначається положенням, яким регламентується порядок такої обробки.

Реалізація прав суб'єктів персональних даних повинна бути відновлена після закінчення обставин, через які вона була обмежена.

Суб'єкт персональних даних має право оскаржити рішення щодо обмеження його прав до Уповноваженого Верховної Ради з прав людини або до суду.

16. НАДАННЯ ДОСТУПУ ІНШИМ СУБ'ЄКТАМ ВІДНОСИН, ПОВ'ЯЗАНИХ З ПЕРСОНАЛЬНИМИ ДАНИМИ, ДО ПЕРСОНАЛЬНИХ ДАНИХ ПЕВНОЇ ФІЗИЧНОЇ ОСОБИ АБО ГРУПИ ОСІБ

Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу до персональних даних володільцеві персональних даних.

У запиті зазначають:

- прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи — заявника);
- найменування, місце юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи — заявника);
- прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;
- відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця або розпорядника персональних даних;
- перелік запитуваних персональних даних;
- мета та/або правові підстави для запиту.

Строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження.

Протягом цього строку володілець персональних даних доводить до відома особи, яка подає запит, що запит буде задоволений або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

17. ОПЛАТА ЗА ПОСЛУГИ З НАДАННЯ ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ

Оплата доступу до персональних даних регламентується статтею 19 Закону України «Про захист персональних даних».

- Доступ суб'єкта персональних даних до даних про себе проводиться безоплатно.
- Доступ інших суб'єктів відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи чи групи фізичних осіб може бути платним у разі додержання умов, визначених Законом України «Про захист персональних даних». Оплаті підлягає робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних.
- Розмір плати за послуги з надання доступу до персональних даних органами державної влади визначає Кабінет Міністрів України.
- Органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їхніх повноважень.

18. ПІДСТАВИ ВИДАЛЕННЯ З ДЕРЖАВНИХ БАЗ ДАНИХ ТА РЕЄСТРІВ ВІДОМОСТЕЙ ПРО СУБ'ЄКТА ЗА ЙОГО ЗВЕРНЕННЯМ

Видалення або знищення персональних даних із державних баз і реєстрів можливе лише за чітко визначених законом підстав.

Суб'єкт персональних даних має право пред'являти вмотивовану вимогу про зміну або знищення своїх персональних даних, якщо їх обробляють незаконно або вони невірні.

Видалення або знищення персональних даних з державних баз персональних даних та реєстрів виконують уповноважені суб'єкти лише за наявності визначених підстав Закону України «Про захист персональних даних».

Процедура такого видалення визначається нормативно-правовим актом, що регулює конкретний державний реєстр. Якщо така процедура прямо не передбачена, суб'єкт даних може скористатися своїм правом, передбаченим пунктом 5 частини другої статті 8 Закону України «Про захист персональних даних», — подати вмотивовану вимогу володільцеві із запереченням проти подальшої обробки його персональних даних.

Тобто вимогу має вмотивувати сам суб'єкт.

Крім того, статті 28 і 24 Закону України «Про публічні електронні реєстри» визначають порядок внесення, зміни та видалення інформації з державних реєстрів. Ці норми передбачають, що будь-яке внесення або зміна відомостей у реєстрі має супроводжуватися офіційним повідомленням особи про такі дії, а також правом особи отримати всю наявну про неї інформацію в межах відповідного реєстру.

Отже, видалення даних із державних баз і реєстрів відбувається лише в установленому законом порядку на підставі вимоги

суб'єкта, рішення суду чи припису Уповноваженого Верховної Ради України з прав людини, а також відповідно до процедур, визначених законом про створення конкретного реєстру.

19. ПОРЯДОК ОРГАНІЗАЦІЇ ПРОЦЕСУ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Порядок організації процесу обробки персональних даних — широке поняття та відповідно до законодавства охоплює два ключові елементи:

- зобов'язання володільця вживати організаційних і технічних заходів з метою запобігання їх випадковій втраті або знищенню, незаконній обробці, зокрема незаконному знищенню чи доступові до персональних даних;
- зобов'язання кожного працівника володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних, чи службових, чи трудових обов'язків, так зване зобов'язання конфіденційності.

Володільць самостійно повинен визначати, яких заходів слід вживати з метою забезпечення захисту персональних даних. У будь-якому разі, такі заходи повинні бути пропорційними до потенційних ризиків, пов'язаних з обробкою персональних даних, що проводить володільць (наприклад, обробкою біометричних даних).

Під час організації процесу обробки персональних даних володільці та розпорядники повинні виконати такі дії:

- розробити, підтримувати та періодично переглядати внутрішні документи, спрямовані на забезпечення впровадження принципів захисту даних;
- запровадити ефективні внутрішні процеси та процедури для забезпечення обробки персональних даних відповідно до внутрішніх документів;
- підтримувати ефективне керування ризиками (виявлення, оцінювання, мінімізацію різноманітних внутрішніх і зовнішніх ризиків);
- вести облік операцій обробки персональних даних, щоб мати можливість продемонструвати дотримання вимог щодо захисту даних;

- проводити періодичний огляд усіх впроваджених засобів захисту персональних даних (правил, процедур тощо).

Законодавство та внутрішні документи Національної поліції України детально регламентують порядок обробки персональних даних. Будь-які документи, прийняті з метою обробки персональних даних у Національній поліції України, повинні містити інформацію щодо:

- мети обробки персональних даних;
- складу персональних даних;
- процедури обробки персональних даних.

20. ВНУТРІШНІ ДОКУМЕНТИ ВОЛОДІЛЬЦЯ

Внутрішні документи в галузі захисту персональних даних — це політики, порядки, інструкції, шаблони та інші матеріали, які визначають, як саме орган чи установа працює з персональними даними. Вони потрібні для того, щоб кожен співробітник знав свої обов'язки, а організація могла довести, що діє відповідно до закону.

Такі документи допомагають упроваджувати принципи та вимоги законодавства, систематизувати процеси та підтвердити дотримання принципу підзвітності, тобто здатності продемонструвати законність і прозорість обробки персональних даних.

Внутрішній документ може мати різні цілі та сферу застосування: він може регулювати загальні аспекти обробки персональних даних, конкретні процедури або окремі операції, а також містити зразки та шаблони документів.

Порядок обробки персональних даних — це основний внутрішній документ загального характеру. Він описує підхід та зобов'язання володільця в галузі захисту персональних даних, надає огляд процесів їх обробки та забезпечує відповідність до вимог законодавства.

Порядок обробки персональних даних може охоплювати:

- зобов'язання щодо реалізації принципів захисту даних;
- загальні зобов'язання персоналу, якому доручено обробляти персональні дані;
- права суб'єктів даних;
- алгоритм дій у зв'язку з порушеннями безпеки персональних даних;
- відносини з розпорядниками;
- розкриття даних третім особам;
- керування ризиками та безпеку даних;

- навчання персоналу, процедури перегляду Порядку.

До Порядку додаються інші внутрішні документи, які деталізують окремі процеси, зокрема:

- порядок збереження та видалення даних;
- реєстр операцій з обробки даних;
- реагування на інциденти безпеки;
- оцінка впливу на захист даних;
- оцінка ризиків і впровадження технічних та організаційних заходів.

Також розробляються шаблони та форми документів, наприклад:

- зобов'язання щодо конфіденційності для працівників;
- реєстр порушень безпеки персональних даних;
- шаблон повідомлення про порушення безпеки для наглядового органу чи суб'єкта даних;
- шаблон протоколу обробки персональних даних тощо.

Шаблони та форми допомагають співробітникам уникнути помилок під час виконання обов'язків у галузі обробки персональних даних. Володілець також має встановити для персоналу конкретні обов'язки, щоб забезпечити використання, заповнення та ведення шаблонів і форм у повсякденній діяльності.

21. РЕЄСТР ОПЕРАЦІЙ З ОБРОБКИ ДАНИХ

Органам (підрозділам) Національної поліції України слід вести облік операцій, пов'язаних з обробкою персональних даних, володілець яких вони є.

З цією метою щодо кожного реєстру операцій з обробки персональних даних створюється документ, що містить таку інформацію:

- підстава обробки персональних даних;
- мета обробки персональних даних;
- склад даних, що обробляються;
- категорії суб'єктів, яких персональні дані обробляються;
- строк зберігання персональних даних;
- загальний опис технічних та організаційних засобів забезпечення безпеки персональних даних.

22. ОБОВ'ЯЗКИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДЛЯ ПОСАДОВИХ ОСІБ ВОЛОДІЛЬЦІВ І РОЗПОРЯДНИКІВ ДАНИХ

Ефективний захист персональних даних в організації можливий лише тоді, коли кожен працівник розуміє свою роль і зону відповідальності. Обов'язки в галузі захисту персональних даних залежать від посади, рівня доступу до інформації та характеру виконуваних функцій.

Співробітники Національної поліції України, які безпосередньо беруть участь в операціях з обробки персональних даних (зборі, зберіганні, введенні даних у програмне забезпечення / реєстри / бази даних/інформаційні системи тощо), повинні виконувати додаткові зобов'язання, а саме:

- бути ознайомленими з процесами обробки персональних даних і їхньою роллю та відповідними обов'язками;
- забезпечити наявність правових підстав для збору та подальшої обробки персональних даних, а також відповідність обробки персональних даних до внутрішніх документів, які регламентують питання обробки персональних даних;
- бути в змозі ідентифікувати всі ризики, пов'язані з обробкою та захистом персональних даних;
- розуміти та вміти виконувати інші спеціальні завдання, передбачені внутрішніми документами та інструкціями.

23. ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ ЗАХОДИ, ВПРОВАДЖЕНІ В ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ЩОДО НАЛЕЖНОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Національна поліція України зобов'язана вживати відповідних заходів технічного та організаційного характеру для забезпечення належного рівня безпеки персональних даних.

Запроваджені заходи безпеки повинні ґрунтуватися на аналізі доступних сучасних технологій та організаційних методів захисту інформації, вартості їх імплементації, характеру, масштабів, контексту та цілей обробки персональних даних, а також ризиків, пов'язаних з їх обробкою, випадковим або неправомірним знищенням, втратою, зміною, несанкціонованим розкриттям або доступом до них.

У будь-якому разі, такі заходи повинні відповідати особливостям конкретного процесу обробки персональних даних.

Організаційні заходи охоплюють:

- визначення порядку та рівнів доступу до персональних даних працівників поліції;
- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних та електронного архіву;
- розроблення плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- навчання працівників поліції, які працюють з персональними даними.

Для новоприйнятих на роботу працівників поліції або працівників поліції, які раніше не працювали з персональними даними,

необхідно проводити початкове навчання, перш ніж надати їм доступ до персональних даних.

Навчання завершується підсумковим контролем.

Усі працівники проходять періодичне навчання з питань захисту персональних даних.

Технічні заходи охоплюють:

- псевдонімізацію та шифрування персональних даних;
- безперервне забезпечення конфіденційності, цілісності, доступності персональних даних і стійкості систем обробки;
- забезпечення своєчасного відновлення доступу до персональних даних у разі виникнення аварійної ситуації або порушення безпеки персональних даних;
- запобігання несанкціонованому доступові до персональних даних у ході їх зберігання чи передання;
- створення резервної копії персональних даних.

Тестування, оцінювання та вимірювання ефективності технічних заходів щодо забезпечення безпеки обробки повинні проводитися не рідше ніж один раз на 6 місяців протягом року.

Запровадження тих чи інших технічних або організаційних заходів залежить від особливостей конкретного процесу обробки персональних даних.

24. УПОВНОВАЖЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ АБО ВІДПОВІДАЛЬНА ОСОБА, ЯКА ОРГАНІЗУЄ РОБОТУ, ПОВ'ЯЗАНУ ІЗ ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ЇХ ОБРОБКИ

У центральному органі Національної поліції України має бути визначений уповноважений структурний підрозділ, а в територіальних (зокрема міжрегіональних) органах поліції, закладах та установах, що належать до сфери керування Національної поліції України, відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних під час їх обробки.

Уповноважений структурний підрозділ підпорядковується безпосередньо Голові Національної поліції України.

Інформацію про уповноважений структурний підрозділ або відповідальну особу повідомляють Уповноваженого Верховної Ради України з прав людини.

Уповноважений структурний підрозділ виконує такі завдання: інформує та консультує володільця або розпорядника з питань додержання законодавства про захист персональних даних; взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його Секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних обов'язкові для всіх працівників, які обробляють персональні дані.

25. СИСТЕМА ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

Відповідальна особа не пізніше ніж за 72 години з моменту, коли стало відомо про порушення безпеки персональних даних, зобов'язана повідомити про цей випадок Уповноваженого Верховної Ради України з прав людини, за винятком випадків, якщо порушення може призвести до ризику для прав і свобод фізичної особи та завдати шкоди фізичній особі.

У разі неможливості поінформувати про порушення безпеки персональних даних у визначений строк відповідальна особа зобов'язана повідомити про нього контрольний орган — Уповноваженого Верховної Ради України — без затримки, з моменту, коли стало відомо про порушення, з обґрунтуванням причин недотримання цього строку.

Повідомлення про порушення безпеки персональних даних повинно містити:

- опис характеру порушення з урахуванням категорії та кількості суб'єктів персональних даних, категорії та кількості реєстраційних записів персональних даних, яких стосується порушення;
- контактні дані відповідальної особи або іншої особи, яка може надати додаткову інформацію;
- опис ймовірних наслідків порушення;
- опис заходів, яких ужито або які планує володілець персональних даних для зменшення наслідків витоку.

Національна поліція України зобов'язана документувати будь-які випадки порушення, зокрема факти, пов'язані з ними, їх наслідками та заходами, ужитими для їх усунення.

Національна поліція України регулярно, але не рідше ніж раз на два роки, має переглядати технічні та організаційні заходи, вжиті

для забезпечення належного рівня безпеки персональних даних. За результатами такого огляду готується звіт щодо загального стану забезпечення захисту персональних даних. Звіт має містити рекомендації стосовно необхідності вдосконалення заходів забезпечення безпеки.

Національній поліції України вкрай важливо впроваджувати відповідні технічні та організаційні заходи, щоб уникнути можливих витоків даних.

26. ЗАХИСТ ДАНИХ ЗА ПРИЗНАЧЕННЯМ ТА ЗАХИСТ ДАНИХ ЗА ЗАМОВЧУВАННЯМ

Національна поліція України має впроваджувати технічні та організаційні заходи щодо захисту персональних даних на ранніх етапах проєктування процесів обробки та відповідних систем способом, що гарантуватиме дотримання принципу обробки персональних даних, а саме захист даних за призначенням.

Національна поліція України має забезпечити обробку персональних даних з дотриманням найвищого рівня захисту (наприклад, обробку лише тих даних, які потрібні для досягнення певної мети, дотримання визначеного терміну зберігання, забезпечення обмеженого доступу до даних), щоб персональні дані не були доступними для невизначеної кількості осіб (захист даних за замовчуванням).

Окрім того, Національна поліція України має забезпечити обробку персональних даних способом, що гарантує особам захист прав, якими вони наділені відповідно до Закону України «Про захист персональних даних».

По суті, це вимагає від співробітників Національної поліції України:

- (а) у визначенні способу обробки даних і під час самої обробки вживати належних технічних і організаційних заходів (наприклад, псевдонімізацію) з метою забезпечення наявності необхідних запобіжників на виконання вимог законодавства; та
- (б) вживати належних технічних і організаційних заходів для забезпечення за замовчуванням обробки лише тих персональних даних, які необхідні для досягнення певної мети.

27. ОЦІНКА ВПЛИВУ НА ЗАХИСТ ДАНИХ

Застосування підходу щодо захисту даних за призначенням і захисту даних за замовчуванням тісно пов'язане з вимогою про оцінку впливу на захист даних.

Національна поліція України має оцінити вплив на захист даних до початку такої обробки, у разі:

- широкомасштабної обробки персональних даних;
- проведення профілювання;
- використання нових технологій обробки персональних даних;
- наявності підстав вважати, що характер, обсяг, контекст та цілі обробки, ймовірно, призведуть до настання значного ризику для прав і свобод фізичних осіб.

До оцінки впливу обробки персональних даних на захист персональних даних залучається уповноважений структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних під час їх обробки.

За результатами оцінки впливу складається висновок у письмовій формі, який повинен містити, зокрема:

- детальний опис запланованої обробки персональних даних та її цілей;
- інформацію про оцінку необхідності та пропорційності обробки персональних даних відносно цілей;
- інформацію про оцінку ризиків для прав і свобод суб'єктів персональних даних;
- інформацію про заходи, що передбачені для реагування на ризики, зокрема гарантії, заходи безпеки та механізми для забезпечення захисту персональних даних і демонстрації дотримання вимог законодавства про захист персональних даних.

28. КОНТРОЛЬ ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Контроль за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини.

Контроль полягає в установленні відповідності процесу обробки персональних даних до вимог Конституції України, Закону України «Про захист персональних даних», Типового порядку обробки персональних даних, а також чинним міжнародним договорам України у галузі захисту персональних даних, згоду на обов'язковість яких надала Верховна Рада України.

Уповноважений Верховної Ради України з прав людини має право:

- отримувати і розглядати звернення, після чого ухвалювати відповідні рішення;
- проводити перевірки. Такі перевірки можуть здійснюватися як за зверненнями, так і з власної ініціативи, і можуть мати позаплановий характер;
- вимагати під час проведення перевірки доступу до будь-якої інформації, необхідної для вжиття заходів контролю, навіть якщо такий доступ обмежений;
- затверджувати нормативно-правові акти в галузі захисту персональних даних, коли це передбачено законодавчими приписами, а також звертатися до державних органів, зокрема на місцях, з пропозиціями ухвалити нові нормативно-правові акти чи внести зміни в чинні;
- видавати вимоги, приписи обов'язкового характеру про запобігання або усунення порушень, якщо їх виявлено в галузі захисту даних за результатами проведених перевірок і розгляду звернень;

- у відповіді на звернення роз'яснювати права та обов'язки осіб, надавати рекомендації щодо застосування на практиці законодавства та висновки щодо проєктів кодексів поведінки та змін до них.

29. ПЕРЕВІРКИ ЯК ФОРМА КОНТРОЛЮ ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Контроль Уповноваженого Верховної Ради України з прав людини в галузі захисту персональних даних здійснюється шляхом проведення перевірок фізичних осіб, фізичних осіб — підприємців, підприємств, установ і організацій усіх форм власності, органів державної влади та місцевого самоврядування, що належить до володільців та/або розпорядників персональних даних.

Два типи перевірок Уповноваженого у сфері захисту персональних даних:

- безвиїзна, коли перевірку здійснюють лише на основі наявних документів і фактичних відомостей, а також пояснень, що надали володільці та розпорядники. Таку перевірку проводить керівник та працівники Секретаріату Уповноважено або Представник Уповноваженого;
- виїзна, коли перевірку проводять за місцем перебування відповідної фізичної або юридичної особи, чи місцем проведення обробки персональних даних.

Перевірки можуть бути планові, затверджені відповідним планом Уповноваженого, та позапланові, що використовуються як засіб реагування на звернення громадян, отримання інформації або реагування на безпосереднє виявлення порушень захисту персональних даних.

Уповноважений або призначені ним посадові особи мають багато прав щодо проведення перевірок. Вони можуть вільно заходити до об'єкта перевірки, діставати доступ до будь-якої інформації та документів володільців й розпорядників, зокрема й до персональних даних, які вони обробляють.

За результатами перевірок можна сформулювати три види документів:

- акт перевірки, в якому зазначають встановлені факти та надають висновок про результати перевірки, зокрема про наявність або ні порушень;
- припис Уповноваженого, яким він вимагає усунути порушення та відновити порушені права. Припис формують на підставі акта перевірки з виявленими порушеннями захисту персональних даних. Припис обов'язковий для виконання і містить відомості про заходи, яких необхідно вжити, щоб усунути порушення, термін їх виконання та строк інформування Уповноваженого про усунення порушень.

Проте припис може передбачати й жорсткі заходи, такі як призупинення або повне зупинення обробки персональних даних;

- протокол про адміністративні правопорушення, який складає Уповноважений або призначені ним посадові особи, та визначає порушення, виявлені в ході перевірки. Зокрема, це стосується тих правопорушень у галузі захисту персональних даних, за які передбачено адміністративну відповідальність.

30. ДЕПАРТАМЕНТ МОНІТОРИНГУ ДОДЕРЖАННЯ ІНФОРМАЦІЙНИХ ПРАВ СЕКРЕТАРІАТУ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ

Забезпечення реалізації повноважень Уповноваженого Верховної Ради України з прав людини щодо здійснення парламентського контролю за дотриманням прав людини і громадянина на захист персональних даних, передбачених статтею 23 Закону України «Про захист персональних даних», покладено на Департамент моніторингу дотримання інформаційних прав Секретаріату Уповноваженого Верховної Ради України з прав людини відповідно до розподілу функціональних обов'язків.

Основним завданням департаменту є забезпечення реалізації повноважень Уповноваженого під час здійснення парламентського контролю за дотриманням прав людини і громадянина у сфері інформаційних прав, зокрема права на звернення, доступу до публічної інформації та захисту персональних даних.

Основними завданнями департаменту є:

- забезпечення розгляду звернень, листів, повідомлень, надання рекомендацій;
- здійснення нормативно-правового забезпечення інформаційних прав, організація та участь у здійсненні нормотворчої роботи, опрацювання, проведення юридичної експертизи проєктів нормативно-правових актів;
- здійснення моніторингу та перевірок стану дотримання прав людини і громадянина у сфері дотримання інформаційних прав;
- забезпечення поновлення порушених прав людини і громадянина;

- забезпечення виконання міжнародних зобов'язань України щодо імплементації міжнародних правових норм та стандартів, зокрема законодавства Європейського Союзу, у сфері додержання інформаційних прав;
- забезпечення просвітницької роботи.

31. ПІДВИЩЕННЯ ОБІЗНАНОСТІ ГРОМАДСЬКОСТІ, ПРЕДСТАВНИКІВ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ ТА БІЗНЕСУ В ГАЛУЗІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Україна робить важливі кроки з метою підвищення обізнаності представників органів державної влади в галузі захисту персональних даних.

Спеціалізований курс «Захист персональних даних» для державних службовців та осіб, які працюють з персональними даних, розробили Уповноважений Верховної Ради України з прав людини та Офіс Ради Європи в Україні в рамках Спільного проєкту «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Офісу Омбудсмана у захисті прав людини», співпрацюючи зі студією онлайн-освіти «EdEra» (<https://study.ed-era.com/uk/courses/course/372>).

Міністерство цифрової трансформації України запустило освітній серіал під назвою «Персональні дані». Ці відеоматеріали допомагають навчати людей бути обачливими, розміщуючи особисту інформацію в інтернеті, розуміти свої права щодо захисту персональних даних та як діяти в разі порушення цих прав (<https://osvita.diia.gov.ua/courses/personaldata>).

Міністерство цифрової трансформації України також розробило інструментарій, що має допомогти компаніям забезпечити захист персональних даних. Ініціатива спрямована на зменшення кількості порушень у галузі персональних даних. Інструментарій охоплює спеціально розроблений тест для оцінювання відповідності компаній до вимог законодавства щодо захисту персональних даних (<https://business.diia.gov.ua/service/test/test-dlia-kontrolera-personalnykh-danykh-za-zakonodavstvom-yes>).

32. ВІДПОВІДАЛЬНІСТЬ І САНКЦІЇ

Відповідальність та санкції за порушення законодавства про захист персональних даних передбачені Законом України «Про захист персональних даних», а саме адміністративна та кримінальна відповідальність за недотримання законодавства про захист персональних даних. Така відповідальність додатково викладена в Кодексі про адміністративні правопорушення та Кримінальному кодексі України. Суб'єкт даних може вимагати компенсації в суді за шкоду, заподіяну внаслідок порушення положень законодавства про захист персональних даних.

На практиці до переліку порушень потрапляє здебільшого незаконне передання персональних даних (чи незаконний доступ з боку третіх осіб). Здебільшого осіб притягують до відповідальності на підставі частини четвертої ст. 188–39 КУПАП за незаконного передання персональних даних третім особам.

Кримінальна відповідальність настає у разі порушення статті 182 Кримінального кодексу України, присвяченої порушенню недоторканності приватного життя. Порушення приватного життя полягає в неправомірному втручанні в особисте чи сімейне життя особи, які можуть проявитись у таких формах: 1) незаконне збирання конфіденційної інформації про особу; 2) незаконне зберігання такої інформації; 3) незаконне її використання; 4) незаконне поширення конфіденційної інформації про особу; 5) поширення її в публічному виступі, творі, що публічно демонструється, або в засобах масової інформації. Всі ці дії утворюють склад злочину, передбаченого ст. 182, лише в разі, якщо вони робляться без згоди особи, якої вони стосуються.

33. ПОРЯДОК ДІЙ СПІВРОБІТНИКА НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У РАЗІ, ЯКЩО ПІД ЧАС ЗАТРИМАННЯ АБО СКЛАДАННЯ АДМІНІСТРАТИВНОГО ПРОТОКОЛУ ОСОБА ВІДМОВЛЯЄТЬСЯ НАДАВАТИ ПЕРСОНАЛЬНІ ДАНІ

Затримання особи — захід забезпечення як адміністративного, так і кримінального провадження, що застосовується на підставі та в порядку, визначених КУпАП та КПК України¹.

Як захід забезпечення провадження у справах про адміністративні правопорушення адміністративне затримання полягає в примусовому короткочасному обмеженні свободи дій і пересування правопорушника.

З метою встановлення особи у разі скоєння особою зазначених адміністративних правопорушень поліцейський має право затримати її за наявності підстав, визначених у статті 260 КУпАП.

З метою складення протоколу про адміністративне правопорушення в разі неможливості скласти його на місці скоєння правопорушення, якщо складення протоколу обов'язкове, порушник може бути доставлений у поліцію.

І поліцейський зобов'язаний негайно повідомити особу зрозумілою для неї мовою підстави затримання, роз'яснити право отримувати медичну допомогу, давати пояснення, оскаржувати затримання, повідомити інших осіб про затримання, захищати себе особисто та користуватися правовою допомогою захисника.

Адміністративне затримання правопорушника може тривати не довше ніж три години, відлік яких розпочинають з моменту фактичного затримання особи.

1 https://www.navs.edu.ua/files/naukova-diyalnist/naukovi-laborator/lab_nni1/2023/dovidnyk_politseiskoho.pdf.

34. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ОСІБ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Відповідно до положень статті 104 Кримінального процесуального кодексу України, що встановлює вимоги щодо оформлення протоколів, у вступній частині протоколу мають бути зазначені прізвища, імена, по батькові, дати народження, місця проживання всіх осіб, присутніх під час проведення процесуальної дії.

***Приклад.** На практиці, у протоколах слідчих дій, особливо в протоколах допиту учасників кримінального провадження, часто зазначають також контактні номери телефонів, відомості про документ, за допомогою якого встановлено особу — учасника слідчої дії тощо, хоча законодавство прямої вимоги про це не містить. Таку інформацію також можна віднести до персональної, бо вона може сприяти ідентифікації особи — учасника кримінального провадження. А отже, вся вище перелічена персональна інформація про будь-якого учасника кримінального провадження підлягає захистові.*

Способи захисту персональних даних осіб у кримінальному провадженні:

1. Будь-яка інформація в кримінальному провадженні захищена таємницею досудового розслідування.

Відповідно до ч. 1 ст. 222 КПК відомості досудового розслідування можна розголошувати лише з письмового дозволу слідчого або прокурора і тим обсягом, яким вони визнають можливим. Згідно із ч. 2 вказаної статті, слідчий, прокурор попереджає осіб, яким стали відомі відомості досудового розслідування, у зв'язку з участю в ньому, про їхній обов'язок не розголошувати таких відомостей без його дозволу. Незаконне розголошення відомостей до-

судового розслідування тягне за собою кримінальну відповідальність, встановлену законом.

Відповідно до положень Кримінального кодексу України, така відповідальність установлена статтею 387 «Розголошення даних оперативно-розшукової діяльності, досудового розслідування».

2. До постраждалих осіб можна застосовувати положення Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», якщо вони набули статусу свідка, потерпілого чи іншого учасника кримінального провадження.

35. ТРАНСКОРДОННЕ ПЕРЕДАННЯ ПЕРСОНАЛЬНИХ ДАНИХ

Закон України «Про захист персональних даних» приділяє значну увагу питанню транскордонного передавання персональних даних. Передання персональних даних іноземним суб'єктам відносин проводиться за умови, якщо інша держава забезпечує належний захист персональних даних у випадках, передбачених законом або міжнародним договором України. Коли персональні дані передають з України володільцеві, розпорядникові або іншим одержувачам у третіх країнах або міжнародним організаціям, держава-одержувач повинна забезпечити належний рівень захисту.

В українському законодавстві визначено перелік держав, які гарантують належний рівень захисту персональних даних (додаток до постанови Кабінету Міністрів України від 16 серпня 2022 р. № 910²). До цього переліку внесено насамперед держави — члени Європейського економічного простору, який охоплює Європейський Союз та країни, які входять до Європейської асоціації вільної торгівлі, а також держави — учасниці Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних.

У разі транскордонного передавання персональних даних необхідно зважати також на особливості окремих національних законодавств, бо Кабінет Міністрів України може встановлювати перелік інших держав, які задовольняють необхідні критерії.

2 <https://zakon.rada.gov.ua/laws/show/910-2022-%D0%BF#n12>.

36. ЄВРОПОЛ

Європол — це правоохоронний орган ЄС зі штаб-квартирою в місті Гаазі та національними підрозділами Європолу в кожній з держав — членів ЄС.

Мета Європолу — надання допомоги в запобіганні та розслідуванні організованої злочинності та тероризму. Він робить це шляхом обміну інформацією та виконання ролі інформаційного центру ЄС, аналізу розвідувальної інформації та оцінювання загроз.

Для досягнення своїх цілей Європол створив Інформаційну систему Європолу (Europol Information System — EIS), яка надає державам-членам базу даних для обміну розвідувальними даними та інформацією.

Інформаційна система Європолу може використовуватися для доступу до даних, що стосуються: осіб, які підозрювані або засуджені за скоєння кримінального правопорушення, що входить до компетенції Європолу або осіб, факти щодо яких вказують на те, що вони готуються скоїти такі правопорушення.

Передавання персональних даних третім країнам або міжнародним організаціям дозволяється, лише якщо Європейська Комісія вирішить, що відповідна держава або міжнародна організація забезпечує відповідний рівень захисту даних або якщо існує міжнародна угода чи угода про співробітництво. Весь обмін інформацією ведеться через Мережу забезпечення обміну інформацією (SIENA)³.

3 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf.

37. СПІВРОБІТНИЦТВО МІЖ УКРАЇНОЮ ЄВРОПОЛОМ

Україна та Європейський поліцейний офіс співпрацює на підставі Угоди між Україною та Європейським поліцейним офісом про оперативне та стратегічне співробітництво від 14 грудня 2016 року. За угодою, співробітництво органів поширюється на всі сфери злочинності, що входять до компетенції Європолу, зокрема пов'язані з ними злочини. Основне завдання співпраці — обмін інформацією.

За загальним правилом, взаємодія України з Європолом ведеться через Департамент міжнародного співробітництва Національної поліції України.

Завдяки співпраці українських правоохоронних органів, Європолу та правоохоронних органів інших країн проведено масштабну кількість різних операцій. Зокрема це стосується: нелегального обігу вогнепальної зброї, вилучення підроблених товарів та готівки, зупинення діяльності злочинних груп та ряд інших⁴.

4 https://golaw.ua/ua/insights/publication/shho-potribno-znati-pro-yevropol-ta-jogo-spivpracyu-z-ukrayinoyu/?fbclid=IwAR0h5TIXTou0DBrVcrTtJfIBsH2uS3Rpk6T_TlrwUMskscKVamOKTcMJWbE.

38. ДИРЕКТИВА (ЄС) 2016/680

Директива (ЄС) 2016/680 про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади з метою запобігання, розслідування, виявлення кримінальних правопорушень і притягнення до відповідальності за їх скоєння або виконання кримінальних покарань та про вільне переміщення таких даних спрямована на захист персональних даних, зібраних та підданих обробці для цілей кримінального правосуддя, зокрема:

- запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення або виконання кримінальних покарань, серед іншого боротьбу із загрозами громадській безпеці та їм запобігання;
- виконання кримінальних покарань;
- справи, у яких поліція або інші правоохоронні органи діють для підтримки закону та захисту від загроз громадській безпеці та засадничим правам суспільства, які можуть становити кримінальне правопорушення, а також запобігання таким загрозам.

Директива (ЄС) 2016/680 захищає різні категорії персональних даних людей, залучених до кримінального провадження, як-от свідків, інформаторів, потерпілих, підозрюваних і співучасників. Поліція та органи кримінальної юстиції зобов'язані дотримуватися положень Директиви (ЄС) 2016/680 за будь-якої обробки персональних даних з правоохоронними цілями як щодо особистого, так і матеріального обсягу Директиви (ЄС) 2016/680.

Директива (ЄС) 2016/680 застосовується як до обробки даних на національному рівні, так і до транскордонної обробки між поліційними та судовими органами держав-членів, а також до міжнародного передавання даних компетентними органами до третіх країн та міжнародних організацій⁵.

5 https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf.

39. ВІДЕОМОНІТОРИНГ СТАНУ ПУБЛІЧНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ СИСТЕМ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

Відеомоніторинг із використанням технологій розпізнавання обличчя застосовується для підвищення рівня публічної безпеки, запобігання злочинам та розшуку осіб, які можуть бути причетними до правопорушень. Такі системи аналізують зображення з камер спостереження і порівнюють їх із базами даних, щоб ідентифікувати осіб.

Водночас застосування таких технологій пов'язане з обробкою біометричних персональних даних, що належать до спеціальних категорій і потребують особливо суворого захисту. Тому використання систем розпізнавання обличчя можливе лише на законних підставах, з чітко визначеними цілями і з дотриманням принципів пропорційності, мінімізації даних та прозорості.

У Європейському Союзі 1 серпня 2024 року набув чинності акт, що регулює правила в галузі штучного інтелекту (Artificial Intelligence Act). Акт ЄС про штучний інтелект забороняє використання систем віддаленої біометричної ідентифікації в режимі реального часу в публічно доступних місцях для цілей правоохоронних органів. Виняток робиться, тільки коли таке використання суворо необхідне для досягнення однієї з таких цілей:

- цільового пошуку конкретних жертв викрадення, торгівлі людьми або сексуальної експлуатації, а також пошук зниклих осіб;
- запобігання конкретній, значній та неминучій загрозі життю або фізичній безпеці осіб, а також реальній та наявній або реальній та передбачуваній загрозі терористичного нападу;
- локалізації або ідентифікації особи, яку підозрюють у скоєнні кримінального правопорушення, з метою проведення кримінального розслідування або переслідування, або виконання кримінального покарання за правопорушення, за які в дер-

жаві — члені ЄС передбачено позбавлення волі або затримання на строк не менше ніж чотири роки.

У разі впровадження технологій розпізнавання обличчя необхідно мати детальні законодавчі правила, які визначають обсяг, мету та порядок використання таких технологій, а також механізми контролю і захисту від зловживань. Потреба в таких запобіжниках особливо важлива, якщо йдеться про використання технологій у реальному часі, коли дані збирають і обробляють негайно.

Крім того, громадяни мають право бути поінформованими про місця, де встановлені камери, мету збору даних, строки їх зберігання та орган, який відповідає за їх обробку. Це вимога як національного законодавства, так і міжнародних стандартів у галузі захисту персональних даних.

40. ЯК ЗАБЕЗПЕЧИТИ КОНФІДЕНЦІЙНІСТЬ ДАНИХ ПІД ЧАС ВІДЕОФІКСАЦІЇ?

Питання конфіденційності даних під час відеофіксації регламентує Інструкція із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису, що передбачає застосування працівниками поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису.

Під час виконання своїх повноважень поліцейським забороняються:

- самовільне видалення відеозаписів з носіїв відеозапису, заміна цих носіїв, зміна їх системної дати та часу;
- примусове вимкнення відеореєстраторів, зокрема на вимогу сторонніх осіб;
- перешкоджання проведенню фото- і кінозйомки, відеозапису;
- використання носіїв відеозапису у випадках, не пов'язаних з виконанням ними повноважень поліції;
- копіювання, передавання інформації з відповідних носіїв стороннім особам.

Вивантаження відеозаписів з карт пам'яті портативних відеореєстраторів і відеореєстраторів, установлених на службових транспортних засобах, БпЛА, на сервер зберігання відеозаписів відбувається шляхом приєднання карти пам'яті до спеціального обладнання в автоматичному режимі за допомогою спеціального програмного забезпечення або іншим способом, що визначив виробник для такого сервера.

Відеозаписи автомобільних і стаціонарних систем зберігаються на сервері способом, який визначив виробник.

Контроль за використанням технічних приладів і технічних засобів, що мають функцію фото- і кінозйомки, відеозапису, веде відповідальна особа, за інформацією, отриманою з їх допомогою, — безпосередньо керівник органу, підрозділу поліції.

Дозвіл на копіювання та видачу відеозаписів надається відповідальній особі лише за рішенням керівника цього органу, підрозділу поліції.

Копіювання та видача відеозапису проводить відповідальна особа на підставі відповідного письмового доручення керівника органу, підрозділу поліції або особи, яка виконує його обов'язки.

У разі копіювання та видачі відеозапису роблять помітку в Журналі обліку копіювання та видачі відеозаписів зі стаціонарної системи або в Журналі обліку.

Відеозаписи або копії з них можуть бути надані за вмотивованими запитами органів державної влади, органів досудового розслідування, прокуратури, слідчого судді та суду, поліцейського та інших осіб у порядку, передбаченому законодавством України.

Передавання відеозаписів, отриманих з портативних і відеореєстраторів, установлених на службових транспортних засобах, БпЛА, автомобільних та стаціонарних систем для використання засобами масової інформації, а також поширення в інтернеті, відбувається з дозволу керівника органу, підрозділу поліції з дотриманням Закону України «Про захист персональних даних». Таке передавання робиться лише з метою забезпечення безпеки та захисту інтересів громадян, суспільства і держави, а також з метою захисту гідності та честі працівника поліції.

Відеозаписи працівникам органу, підрозділу поліції видають у тому вигляді, в якому вони були збережені на док-станції, — без коригування. Перегляд, аналіз відеозапису робить працівник поліції, якому він виданий у встановленому цією Інструкцією порядку для виконання покладених на нього завдань у межах його повноважень.

41. ЧИ МАЄ ПРАВО ПОЛІЦЕЙСЬКИЙ ВЕСТИ ФОТО-, ВІДЕОФІКСАЦІЮ ДОКУМЕНТІВ АБО ОБЛИЧЧЯ ОСОБИ НА МІСЦІ ПОДІЇ?

Згідно з пунктом дев'ять частини першої статтею 31 Закону України «Про національну поліцію України» поліція може застосовувати превентивні заходи: «застосування технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису».

Відповідно до статті 40 Закону України «Про національну поліцію України»: «Поліція для виконання покладених на неї завдань та здійснення повноважень, визначених законом, може застосовувати такі технічні прилади, технічні засоби та спеціалізоване програмне забезпечення: фото- і відеотехніку, у тому числі техніку, що працює в автоматичному режимі, технічні прилади та технічні засоби з виявлення та/або фіксації правопорушень».

Питання проведення фото-, відеофіксації в діяльності Національної поліції України регламентується Наказом № 1026 «Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису».⁶

Інструкція із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису передбачає застосування працівниками поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, ведеться з метою:

- запобігання, виявлення або фіксування правопорушення;

6 <https://zakon.rada.gov.ua/laws/show/z0028-19#Text>.

- охорони громадської безпеки та власності;
- забезпечення безпеки осіб;
- забезпечення публічної безпеки і порядку.

42. ЯКІ ВИМОГИ ІСНУЮТЬ ЩОДО ВИКОРИСТАННЯ МОБІЛЬНИХ ЗАСТОСУНКІВ (ВАЙБЕРУ, ВАЦАПУ) ДЛЯ ОБМІНУ СЛУЖБОВОЮ ІНФОРМАЦІЄЮ?

Питання обміну інформацією в установі регламентує Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну (затверджено Постановою Кабінету Міністрів України від 17 січня 2018 р. № 55⁷).

Інформаційний обмін між працівниками установ ведеться з використанням службової електронної пошти. Службова електронна пошта — адреса електронної пошти працівника установи, сформована з використанням доменного імені в домені gov.ua для обміну управлінською інформацією, яка не має юридичної сили.

Також інформаційний обмін між працівниками установи може вестися за допомогою інших засобів електронних комунікацій за рішенням керівника установи.

Інформаційний обмін ведеться з метою:

- попереднього погодження редакції проєктів спільних електронних документів, зокрема співрозроблення проєктів актів;
- доведення управлінської інформації до відома, зокрема про плани та роботу відповідних установ;
- інформування про ухвалені установою управлінські рішення;
- з'ясування стану опрацювання установою електронних документів, що надійшли на її розгляд.

Інформація з листування службовою електронною поштою може використовуватися для підтвердження виконаних дій.

7 <https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text>.

Проте важливо зауважити: «інформаційний обмін службовою електронною поштою не допускається щодо інформації з обмеженим доступом».

Використання служб для обміну миттєвими повідомленнями (телеграму, вацапу, месенджеру фейсбуку,, сигналу) для цілей передавання службової інформації в органах державної влади не допускається.

43. КЛЮЧОВІ ПРАВОВІ ПОЗИЦІЇ ВЕРХОВНОГО СУДУ В СПРАВАХ, ЩО СТОСУЮТЬСЯ ПРИНЦИПІВ І ПІДСТАВ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Принцип законності має особливо чіткі форми вираження щодо діяльності суб'єктів владних повноважень. Тут повинна, безумовно, діяти формула припису частини другої статті 19 Конституції України, відповідно до якої органи державної влади та органи місцевого самоврядування, їхні посадові особи, зобов'язані діяти лише на підставі, в межах повноважень та способом, що передбачені Конституцією та законами України. Дотримання цієї вимоги особливо важливе, коли йдеться про обмеження прав людини, зокрема, про втручання в приватне життя особи та захист персональних даних. Тут показовою може бути справа № 804/4069/17, у якій Верховний Суд досить чітко наголосив на необхідності вкрай чіткого застосування формули «якщо не заборонено, то дозволено».

На підставі закону обробка персональних даних ведеться в межах реалізації наданих органам публічної влади повноважень. Одержання згоди від суб'єкта персональних даних на обробку його персональних даних не вимагається у разі витребування таких даних суб'єктом владних повноважень у межах наданих йому повноважень. Така позиція не тільки поширена в діяльності органів державної влади та органів місцевого самоврядування, але й підтверджується судовою практикою у справі Верховного Суду № 520/4861/19⁸.

8 <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/e777089b-6b99-44f3-b3cb-1412226eb87c/content>.

44. РЕФОРМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

З метою реалізації міжнародних зобов'язань України в галузі захисту персональних даних та реформи захисту персональних даних в Україні розроблено законопроекти № 8153 «Про захист персональних даних» та № 6177 «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації». Обидва законопроекти покликані імплементувати в національне законодавство вимоги Конвенції 108+, Регламенту (ЄС) 2016/679 та Директиви (ЄС) 2016/680.

Законопроект «Про захист персональних даних» № 8153 закладає основи для якісно нового підходу до захисту персональних даних в Україні та, зокрема, передбачає:

- увідповіднення термінології в галузі захисту персональних даних до європейських стандартів;
- деталізацію стандартів, принципів і підстав обробки персональних даних;
- підвищення рівня відповідальності контролерів та операторів даних за обробку персональних даних суб'єктів;
- розширення та деталізацію прав суб'єктів даних, зокрема права на забуття, мобільність даних тощо;
- запровадження оцінки впливу на захист даних та принципів «захист даних за замовчуванням» і «захист даних за призначенням», які гарантують високий рівень приватності на всіх етапах обробки даних;
- обов'язкове інформування наглядового органу про порушення безпеки персональних даних протягом 72 годин;
- вимоги до призначення відповідальної особи з питань захисту персональних даних;
- врегулювання транскордонного передавання даних з дотриманням належного рівня захисту;

- введення ефективних фінансових санкцій за порушення законодавства про захист персональних даних.

Для повноцінного функціонування системи захисту персональних даних в Україні важливе створення незалежного наглядового органу відповідно до стандартів ЄС та Ради Європи.

Законопроект «Про Національну комісію з захисту персональних даних і доступу до публічної інформації» № 6177 визначає:

- процедуру створення, функціонування та структура Національної комісії;
- повноваження Національної комісії;
- порядок провадження та перевірок Національної комісії;
- структура апарату Національної комісії, в якій утворюється спеціальний структурний підрозділ — служба інспекторів Національної комісії;
- окремий порядок притягнення до дисциплінарної відповідальності інспекторів та службовців Національної комісії;
- порядок відкриття та провадження Національної комісії;
- порядок виконання рішень Національної комісії, зокрема оплата штрафу в разі його накладення Національною комісією;
- порядок оскарження рішень, дій чи бездіяльності Національної комісії до суду;
- порядок взаємодії із суб'єктами контролю;
- порядок взаємодії Національної комісії з іншими органами державної влади;
- порядок громадського контролю за діяльністю Національної комісії.

Створення незалежного контрольного органу в галузі захисту персональних даних і доступу до публічної інформації дасть змогу забезпечити належний контроль за дотриманням права на захист персональних даних і права на доступ до публічної інформації як органами публічної влади, так і суб'єктами приватного права.

45–50. ПРИКЛАДИ КЕЙСІВ ЩОДО ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІХ ОСІБ

45. Кейс 1. Щодо доступу до персональних даних третіх осіб

Уповноважений Верховної Ради України з прав людини одночасно з народним депутатом України звернулися до Національної поліції України з проханням надати копію висновку службового розслідування / перевірки, що містить відомості про конкретних поліцейських, цивільних осіб та/або обставини досудового розслідування. Чи є підстави для надання такої копії з огляду на обмеження, встановлені законодавством про захист персональних даних, зокрема статті 7, 10 Закону України «Про захист персональних даних» та вимог кримінального процесуального законодавства?

Відповідно до статті 7 Закону України «Про захист персональних даних», обробка персональних даних без згоди суб'єкта заборонена, за винятком випадків, прямо передбачених законом. Стаття 10 цього ж Закону встановлює заборону розголошення персональних даних третім особам без згоди, крім випадків, коли такий доступ прямо надано законом. Крім того, стаття 222 Кримінального процесуального кодексу України визначає, що відомості досудового розслідування становлять таємницю і можуть бути розголошені лише в межах та порядку, передбаченому КПК.

Водночас, відповідно до статті 13 Закону України «Про Уповноваженого Верховної Ради України з прав людини», Уповноважений має право безперешкодно отримувати будь-які документи, зокрема ті, що містять персональні дані чи іншу інформацію з обмеженим доступом, якщо це необхідно для виконання його повноважень із захисту прав людини. Це означає, що його запит

має законні підстави і не порушує обмеження щодо захисту персональних даних чи таємниці досудового розслідування.

Щодо народного депутата, то Закон України «Про статус народного депутата України» (статті 16, 24) гарантує йому право на депутатське звернення. Проте це право не означає автоматичного доступу до персональних даних чи матеріалів досудового розслідування. Депутат може отримати лише загальну або знеособлену інформацію, якщо інше не передбачено спеціальною нормою закону.

Висновки:

- Уповноважений Верховної Ради України з прав людини (стаття 13 Закону «Про Уповноваженого Верховної Ради України з прав людини») має право на отримання копії документа, навіть якщо він містить персональні дані та інформацію досудового розслідування.
- Народний депутат (статті 16, 24 Закону «Про статус народного депутата України») не має підстав для отримання такої копії без знеособлення даних чи спеціальної законної норми.
- Національна поліція України повинна надати копію документа саме Уповноваженому, посилаючись на його повноваження, але не депутатові.

46. Кейс 2. Щодо доступу до персональних даних третіх осіб

Адвокат, який діє в інтересах чоловіка (на підставі усної домовленості або довіреності), звернувся до Національної поліції України із запитом про отримання інформації, зокрема щодо притягнення дружини до адміністративної та/або кримінальної відповідальності, необхідної адвокату для звернення до суду з питань позбавлення дружини батьківських прав. Чи є законні підстави для надання такої інформації? Які документи (зокрема, належним чином оформлена довіреність чи договір про надання правової

допомоги, усна домовленість) мають бути додані до запиту? Як діяти, якщо адвокат покликається на усну домовленість?

У цій ситуації ключовий є баланс між правом на доступ до інформації в інтересах клієнта (чоловіка) та правом дружини на захист персональних даних і таємницю досудового розслідування.

Чи є підстави для надання такої інформації?

Ні, у загальному випадку поліція не має права надавати третім особам (зокрема адвокатам) інформацію про притягнення особи (дружини) до адміністративної чи кримінальної відповідальності без належних правових підстав.

Причини:

1. Це персональні дані дружини, а отже, діє Закон України «Про захист персональних даних», зокрема статті 7 і 10.
2. Інформація може стосуватися таємниці досудового розслідування (якщо йдеться про кримінальне провадження), застосовується ст. 222 КПК України.
3. Нема законного інтересу: навіть якщо адвокат діє в інтересах чоловіка, сам по собі факт шлюбу або наміру звернутися до суду щодо позбавлення батьківських прав не створює автоматичного права на доступ до такої інформації без згоди дружини чи рішення суду.

Які документи мають бути додані до запиту?

Якщо запит подає адвокат, він має додати:

1. Ордер (форма №1) — підтвердження повноважень на представництво особи згідно зі статтею 26 Закону України «Про адвокатуру та адвокатську діяльність».
2. Договір про надання правової допомоги між адвокатом і клієнтом (чоловіком).
3. Нотаріальну довіреність — не обов'язково, але вона може деколи бути додатковим підтвердженням, якщо адвокат діє не як захисник, а як представник у цивільному процесі.

4. Мотивацію правового інтересу — обґрунтування, чому ця інформація необхідна для захисту прав клієнта (наприклад, для підготування позову до суду про позбавлення батьківських прав).

Якщо адвокат посилається на усну домовленість, цього недостатньо.

Поліція **не має права** надавати персональні дані третьої особи (дружини), якщо:

- немає документів, що підтверджують повноваження адвоката;
- нема згоди суб'єкта персональних даних (дружини);
- не надано рішення суду або нема іншої прямої законної підстави.

Як правильно діяти органу поліції в цьому разі:

1. Відмовити в наданні інформації, якщо:
 - адвокат не надав ордер / договір;
 - нема належного обґрунтування правового інтересу;
 - запит містить дані щодо іншої особи (дружини) без її згоди чи рішення суду.
2. Письмово повідомити адвоката, що:
 - відповідно до законодавства, надання персональних даних можливе лише за наявності законних підстав;
 - усна домовленість не підтверджує представництво;
 - порекомендувати звернутися до суду із заявою про витребування інформації, якщо вона критична для захисту прав клієнта.

47. Кейс 3. Щодо доступу до персональних даних третіх осіб

Особа запитує інформацію про третіх осіб і зазначає мету та/або правові підстави запиту, що викликають сумніви. Чи передбачено законодавством України можливість перевірки вірогідності заявленої мети обробки персональних даних та правових підстав запиту?

Законодавство України передбачає можливість перевірки вірогідності заявленої мети обробки персональних даних і правових підстав запиту, особливо коли йдеться про надання інформації про третіх осіб.

1. Принцип вірогідності та цільової обробки

Закон України «Про захист персональних даних», зокрема:

- Стаття 6 (Вимоги до обробки): Персональні дані повинні оброблятися з урахуванням визначеної, законної мети та обмежуватися цією метою.
- Стаття 8 (Права суб'єкта персональних даних): Суб'єкт має право знати, хто і з якою метою обробляє його дані.
- Стаття 10 (Обов'язки володільця): Володільць бази персональних даних зобов'язаний не допускати незаконної обробки персональних даних і забезпечити перевірку правових підстав для доступу третіх осіб до таких даних.

2. Можливість перевірки запитів як обов'язок володільця (наприклад, поліції, органу державної влади)

Орган, що володіє персональними даними, має право і обов'язок оцінити:

- Чи запитувач — уповноважена особа (чи дійсно має повноваження представляти інтереси іншої особи, чи діє в межах посадових обов'язків тощо);
- Чи надано належне обґрунтування мети обробки;
- Чи сумірний запитаний обсяг даних заявленій меті (принцип мінімізації);

- Чи не суперечить заявлена мета закону (наприклад, вимагання, шантаж, неправомірна вигода тощо).

Якщо мета або правові підстави викликають обґрунтовані сумніви, володілець має право відмовити в наданні інформації.

3. Що робити в разі сумнівів?

- Вимагати додаткових документів або пояснення від заявника (довіреності, рішення суду, службового посвідчення, ордера адвоката тощо).
- Уточнити мету запиту, чи дійсно вона правомірна і передбачає доступ до персональних даних третіх осіб.
- Застосовувати принцип «знеособлення» — надання інформації без ідентифікаційних ознак.
- У разі сумнівів відмовити з обґрунтуванням і зазначенням відповідних норм законодавства (наприклад, ст. 22 Закону про захист персональних даних).

48. Кейс 4. Щодо доступу до персональних даних третіх осіб

Журналіст звернувся до Національної поліції України із запитом про надання інформації щодо прізвищ, імен та по батькові, посад поліцейських, залучених до затримання високопосадовця, що мало суспільний резонанс. Існують підозри щодо можливого неправомірного використання цієї інформації. Чи правомірна відмова в наданні такої інформації з посиланням на Закон України «Про захист персональних даних»? Чи передбачає законодавство можливість перевірки такої підозри перед наданням відповіді?

Так, відмова в наданні інформації про конкретних поліцейських у такій ситуації може бути правомірною з посиланням на Закон України «Про захист персональних даних», якщо існують підстави вважати, що запитувана інформація:

- це персональні дані (П.І.Б. + посада конкретної особи — це і є персональні дані);
- може бути використана не за призначенням або призведе до порушення прав / безпеки осіб;
- не інформація з вільним доступом, яку можна надавати без згоди суб'єкта.

1. Що говорить законодавство?

Закон України «Про захист персональних даних»:

- Стаття 2, ч. 2 — до персональних даних належить будь-яка інформація, яка ідентифікує особу, зокрема П.І.Б., посада.
- Стаття 7, ч. 1 — забороняється обробка персональних даних без згоди суб'єкта, крім випадків, встановлених законом.
- Стаття 10 — надавач інформації зобов'язаний перевірити законність підстав доступу.

Закон України «Про доступ до публічної інформації»:

- Стаття 6, ч. 2, п. 5 — доступ обмежується, якщо розголошення персональних даних може завдати шкоди особі.
- Стаття 7 — розпорядник інформації повинен зважити суспільний інтерес та ризики шкоди.

Підставою для обмеження доступу буде також можливість неправомірного використання інформації, навіть у разі журналістського запиту.

2. Чи передбачає закон перевірку добросовісності запиту?

Так. Розпорядник інформації (в цьому разі — поліція) має право і обов'язок оцінити, чи:

- існує суспільний інтерес в оприлюдненні запитаної інформації (і чи переважає він над правом на захист персональних даних);
- може бути заподіяна шкода працівникам поліції внаслідок розголошення П.І.Б. (наприклад, у контексті кримінального переслідування або тиску);

- є ознаки неправомірного інтересу (якщо журналістська діяльність використовується як прикриття).

Тобто закон не лише дозволяє, а зобов'язує перевірити обґрунтованість і добросовісність мети запиту.

Якщо інформація дійсно становить суспільний інтерес, можливе часткове розкриття персональних даних (наприклад, знеособлена інформація, кількість залучених працівників, їх статус — без П.І.Б.).

Рекомендація. У відповіді журналістові можна послатися на обмеження, встановлені ст. 6 Закону «Про доступ до публічної інформації» та ст. 10 Закону «Про захист персональних даних», з поясненням, що П.І.Б. співробітників поліції можуть бути надані лише за умови наявності переважного суспільного інтересу або згоди самих осіб.

49. Кейс 5. Щодо доступу до персональних даних третіх осіб

Особа звернулася до Голови Національної поліції України із запитом про надання інформації щодо конкретного поліцейського, зазначивши лише його прізвище, ім'я та по батькові, а в Національній поліції наявні кілька осіб з такими анкетними даними. Як необхідно діяти в такому разі?

У ситуації, коли запитувач звертається із запитом щодо конкретного поліцейського, вказуючи лише П.І.Б., а в Національній поліції є кілька осіб з такими даними, розпорядник інформації (Нацполіція) має діяти обережно, враховуючи:

1. Принцип правомірності обробки персональних даних

Відповідно до ст. 6, 7, 10 Закону України «Про захист персональних даних» та ст. 6 Закону України «Про доступ до публічної інформації», персональні дані не можуть бути надані, якщо:

- запитувана особа не ідентифікована однозначно;

- існує ризик ненавмисного розголошення інформації про інших осіб (з такими ж П.І.Б.), що порушує їхні права.

2. Як правильно діяти Національній поліції?

Відповісти запитувачеві про неоднозначність ідентифікації:

«У відповіді на Ваш запит повідомляємо, що в Національній поліції України є кілька співробітників із зазначеними анкетними даними (прізвищем, ім'ям та по батькові). Для належного розгляду запиту та запобігання розголошенню персональних даних третіх осіб просимо Вас надати додаткову ідентифікаційну інформацію, що дасть змогу однозначно визначити особу, щодо якої запитується відомості».

Якщо запитувач не надає уточнення, інформація не повинна надаватися, бо це створює ризик порушення прав інших осіб, чий П.І.Б. збігаються.

50. Кейс 6. Щодо доступу до персональних даних третіх осіб

Журналіст звернувся до Національної поліції України із запитом щодо надання інформації про поліцейських окремого стрілецького батальйону, визнаних померлими за рішенням суду, зокрема їхніх П.І.Б. Чи правомірна відмова в наданні такої інформації з посиланням на Закон України «Про захист персональних даних»? Як коректно відмовити в наданні даних?

У цьому разі відмова в наданні П.І.Б. померлих поліцейських може бути неправомірною, якщо вона ґрунтується лише на Законі України «Про захист персональних даних», адже:

1. Закон України «Про захист персональних даних» не поширюється на осіб, що померли, бо:

- Закон регулює обробку персональних даних лише живих осіб.

- Стаття 2 цього Закону означає, що «персональні дані» — це відомості про фізичну особу, яка ідентифікована або може бути ідентифікована».

Померла особа втрачає правосуб'єктність, а отже, не суб'єкт персональних даних у значенні цього закону.

2. Закон України «Про доступ до публічної інформації» застосовується

У запиті журналіста йдеться про публічну інформацію, якою володіє орган державної влади. Відповідно до статті 6 цього закону обмеження доступу до інформації можливе, якщо розголошення може завдати шкоди правам та інтересам третіх осіб, зокрема живих родичів (приклад: право на приватність, спокій, честь і гідність).

3. Коли відмова буде правомірною?

Відмова може бути правомірною, якщо:

- є обґрунтовані підстави вважати, що розголошення імен навіть померлих поліцейських може завдати шкоди інтересам їхніх родичів (наприклад, якщо смерть пов'язана з резонансними подіями, що можуть спричинити ризики для сім'ї);
- інформація офіційно не оприлюднена (не опублікована у відкритих джерелах).

Як коректно відмовити в наданні такої інформації?

Зразок формулювання:

«У відповіді на Ваш запит повідомляємо, що розгляд питання про надання запитуваної інформації, зокрема прізвищ, імен та по батькові поліцейських окремого стрілецького батальйону, які визнані померлими за рішенням суду, потребує врахування положень статті 6 Закону України «Про доступ до публічної інформації».

Зокрема, відповідно до частини 5 цієї статті, не допускається розголошення інформації, яка може завдати шкоди правам та інтересам третіх осіб. Через те що така інформація потенційно може

вплинути на права близьких родичів померлих (особливо у випадках, пов'язаних із резонансними подіями), ухвалено рішення відмовити в наданні персоніфікованих даних.

У разі наявності згоди родичів або рішення суду про розкриття такої інформації, питання може бути розглянуте повторно».

Поліція може надати загальну статистичну або знеособлену інформацію, наприклад:

- кількість таких осіб;
- періоди часу;
- загальна інформація без П.І.Б.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Шевчук О., Венгер В., Кошман А. Дослідження «Аналіз судової практики щодо застосування законодавства України про захист персональних даних». URL: <https://rm.coe.int/report-dp-2021-2web-1680aa5225>.
2. Шевчук О., Олексюк Л., Шинкунене Д. Дослідження «Аналіз європейських моделей незалежних наглядових органів в сфері захисту персональних даних та доступу до публічної інформації». URL: <https://rm.coe.int/analysis-report-2021-ukr-2web/1680a6e81e>.
3. Шевчук О., Тализіна Я. Пам'ятка щодо особливостей обробки та захисту персональних даних осіб, постраждалих від сексуального насильства, пов'язаного з конфліктом. URL: <https://ombudsman.gov.ua/storage/app/media/uploaded-files/pamyatkapdweb.pdf>.
4. Посібник з європейського права у сфері захисту персональних даних. Київ: K.I.C., 2020. 432 с. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf.

НОРМАТИВНО-ПРАВОВІ АКТИ

7. Закон України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
8. Закон України «Про доступ до публічної інформації» № 2939-VI від 13 січня 2011 року. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>.
9. Закон України «Про інформацію» № 2657-XII від 2 жовтня 1992 року. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
10. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>, <https://zakon.rada.gov.ua/laws/show/80732-10#Text>.
11. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>.

12. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.
13. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text.
14. Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data) of 18th May, 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.
15. Регламент Європейського парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.
16. Директива Європейського Парламенту і Ради (ЄС) 2016/680 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за вчинення кримінальних злочинів або виконання кримінальних покарань і про вільний рух таких даних, а також скасування Рамкового рішення Ради 2008/977/JHA. URL: <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>.

SUMMARY

Brochure on protection of personal data in the National Police of Ukraine was prepared as a result of three rounds of consultations on the protection of personal data with representatives of the National Police of Ukraine during the period April-June 2025. Brochure presents a general overview of the processing and protection of personal data in the National Police of Ukraine and provides practical advice on its application. Brochure is focused on practical aspects encountered by the National Police representatives during the performance of their official duties that related to the collection and processing of personal data, documentary support and analytical work, in particular, national and international regulation, principles and standards Council of Europe and the European Union in this area.

www.coe.int

Рада Європи є провідною організацією із захисту прав людини на континенті. Вона нараховує 46 держав-членів, включно з усіма державами-членами Європейського Союзу. Усі держави — члени Ради Європи приєдналися до Європейської конвенції з прав людини — договору, спрямованому на захист прав людини, демократії та верховенства права. Європейський суд з прав людини здійснює нагляд за виконанням Конвенції у державах-членах.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE