Уповноважений
Верховної Ради України
з прав людини

РЕКОМЕНДАЦІЇ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ ЩОДО ДОТРИМАННЯ ПРАВА НА ПРИВАТНІСТЬ ПІД ЧАС ВСТАНОВЛЕННЯ І ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ У ГРОМАДСЬКИХ МІСЦЯХ

Київ
2021

Уповноважений
Верховної Ради України
з прав людини

*Рекомендації підготовлено за участі **Інни Берназюк**, представника Уповноваженого у сфері захисту персональних даних, **Олени Гунько**, завідувача сектору упровадження міжнародних стандартів у сфері захисту персональних даних Департаменту у сфері захисту персональних даних Секретаріату Уповноваженого, **Уляни Шадської**, юриста з питань цифрового законодавства та з залученням експертного сприяння Міжнародного та ібероамериканського фонду адміністративної та державної політики (FIIAPP).*

FIIAPP
COOPERACIÓN ESPAÑOLA

Дизайн розроблено з використанням платформи графічного дизайну Canva.

ЗМІСТ

ПОЗИЦІЯ СЕКРЕТАРІАТУ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ

Системи відеоспостереження стали невід'ємним атрибутом інфраструктури сучасних міст. Камери встановлюються на вулицях, у торговельно-розважальних центрах, ресторанах, всередині та зовні багатоповерхових будинків. Наразі запроваджуються мобільні системи відеоспостереження (дрони). Отримані відеозаписи поєднуються з іншими даними/технологіями і аналізуються для різних цілей. Технології постійно удосконалюються, що в свою чергу призводить до розширення обсягу персональних даних, які обробляються за допомогою таких систем, і все більше впливає на наше приватне життя.

При цьому рівень знань та навичок володільців і розпорядників персональних даних щодо впливу систем відеоспостереження на приватність є недостатнім. Таким чином нерегламентоване використання систем відеоспостереження призводить до порушення прав людини.

Наразі питання обробки персональних даних із використанням систем відеоспостереження чинним законодавством України не врегульовано.

У цьому контексті варто зазначити, що Уповноважений Верховної Ради України з прав людини (далі – Уповноважений) не є суб'єктом законодавчої ініціативи і не приймає рішень щодо законодавчого врегулювання зазначеної сфери. Цією функцією відповідно до чинного законодавства наділені парламент і уряд.

Проте згідно із Законом України «Про захист персональних даних» Уповноважений наділений компетенцією здійснювати моніторинг нових практик, тенденцій, технологій захисту персональних даних, надавати рекомендації щодо практичного застосування законодавства про захист персональних даних в окремих аспектах та роз'яснювати права і обов'язки суб'єктів відносин у сфері захисту персональних даних.

З огляду на це Секретаріатом Уповноваженого було створено цей практичний інструмент, наповнений рекомендаціями й алгоритмами, що має забезпечити дотримання чинного законодавства та міжнародних стандартів у цій сфері з ранніх етапів прийняття володільцем рішення про встановлення систем відеоспостереження.

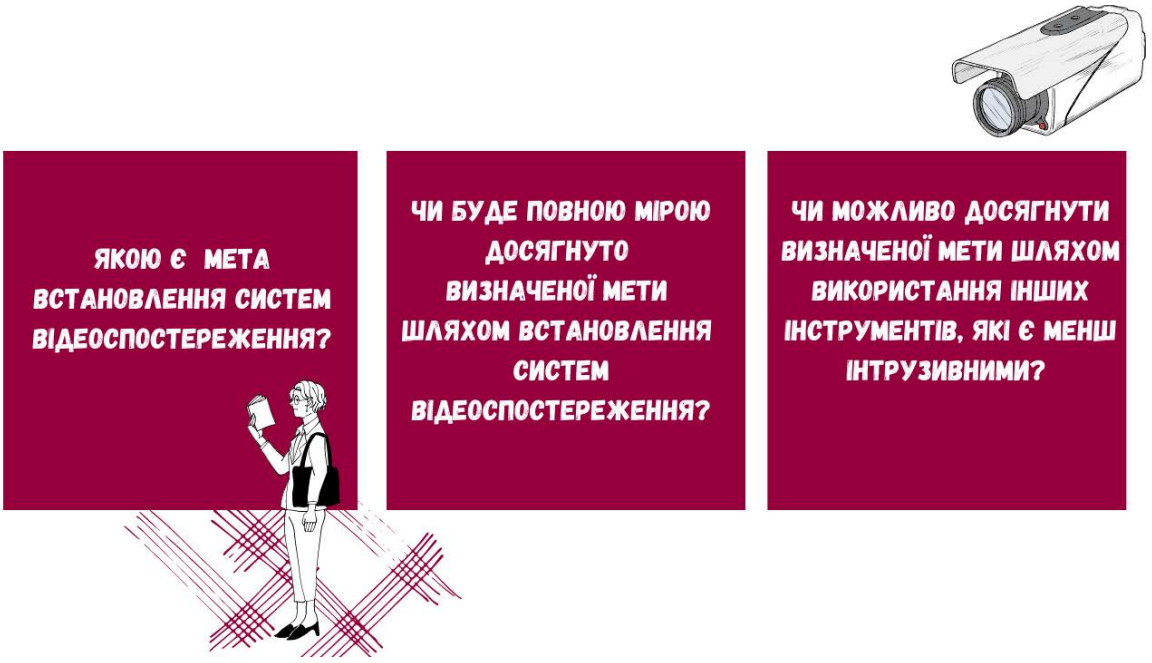
Водночас вивчення окреслених рекомендацій допоможе володільцям та розпорядникам сформувати необхідну внутрішню документацію належним чином.

РОЗДІЛ І. ДІЇ, ЩО НЕОБХІДНО ЗДІЙСНИТИ ДО ПРИЙНЯТТЯ РІШЕННЯ ПРО ВСТАНОВЛЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Крок 1. Оцініть, чи встановлення систем відеоспостереження є пропорційним і відповідним заходом для досягнення певної мети

У частині першій статті 6 Закону України «Про захист персональних даних» визначено, що мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, що регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

З метою дотримання принципу пропорційності до прийняття рішення про встановлення систем відеоспостереження необхідно відповісти на такі запитання:



Варто пам’ятати, що мета має бути сформульована чітко. Занадто загально сформульована мета призводить до порушення принципу мінімізації даних і спричиняє низку ризиків порушення права на приватність.

Чим більше передбачається втручання у приватність внаслідок запровадження певних заходів, тим вагомішими мають бути підстави для його обґрунтування. Тому одразу після визначення мети потрібно оцінити і мінімізувати обсяг персональних даних, обробка яких для цього необхідна.

Крім того, щоб оцінити, чи пропорційним заходом є встановлення систем відеоспостереження для досягнення визначеної мети, необхідно самостійно довести потенційну ефективність такого заходу і його перевагу над тими заходами, що передбачають менше втручання в особисте життя.

Приклад. *Власник магазину одягу помітив випадки викрадення товару і приймає рішення про встановлення систем відеоспостереження з метою запобігання наступним крадіжкам. При цьому довести доцільність застосування такого обсягу втручання у приватне життя йому буде складно, з огляду на те, що наразі існують інші інструменти запобігання крадіжкам, які є менш інтрузивними.*

Отже, власник магазину одягу має розглянути можливість використання спеціальних магнітних кліпсів, що кріпляться на товар і запобігають його викраденню.

Крок 2. Оцініть потенційні ризики для прав суб'єктів персональних даних та розробіть низку заходів для їх мінімізації

Кожна людина має право на приватність та повагу до неї. Згідно зі статтею 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

У статті 8 Закону України «Про захист персональних даних» суб'єктам персональних даних гарантовано низку прав, пов'язаних із захистом приватного життя. Таким чином, до встановлення систем відеоспостереження необхідно подбати про дотримання прав тих, на чию приватність такі заходи реально чи потенційно впливатимуть.

Насамперед оцініть баланс між заходами, обраними для досягнення мети, і рівнем дотримання права на невтручання у приватне життя.

Для цього визначте:

- ✓ *законність підстав для обробки персональних даних, що обробляються з використанням систем відеоспостереження (стаття 11 Закону України «Про захист персональних даних»);*
- ✓ *яким є коло суб'єктів персональних даних, право на приватність яких реально чи потенційно зазнаватиме втручання внаслідок встановлення систем відеоспостереження;*
- ✓ *як повідомлятимуть суб'єктів про вплив встановлених заходів на їхню приватність, про мету втручання і заходи, що вживаються для безпеки їхніх персональних даних;*
- ✓ *як забезпечуватиметься належна якість даних;*

- ✓ *які заходи вживатимуться для мінімізації даних, що обробляються з використанням систем відеоспостереження;*
- ✓ *чи передбачається залучення інших фізичних чи юридичних осіб у якості розпорядників персональних даних та як здійснюватиметься забезпечення їх відповідності вимогам чинного законодавства про захист персональних даних (стаття 4 Закону України «Про захист персональних даних»);*
- ✓ *які організаційні та технічні заходи вживатимуться для запобігання несанкціонованому доступу до персональних даних та які заходи вживатимуться у разі якщо відбувся витік персональних даних;*
- ✓ *чи передбачається транскордонна передача персональних даних і які заходи вживатимуться для того, щоб вона була максимально безпечною (стаття 29 Закону України «Про захист персональних даних»).*

Оцініть потенційні ризики та будь-яку шкоду, що може спричинити передбачувана обробка внаслідок встановлення систем відеоспостереження, зокрема:

- ✓ *перешкоди у реалізації будь-яких прав суб'єктами персональних даних;*
- ✓ *втрату суб'єктами персональних даних контролю над власними персональними даними;*
- ✓ *дискримінацію у будь-якій формі;*
- ✓ *незаконне привласнення цифрової ідентичності;*
- ✓ *шахрайство з викраденими персональними даними;*
- ✓ *завдання шкоди репутації;*
- ✓ *повторну ідентифікацію псевдонімізованих даних;*
- ✓ *будь-яка інша шкода, завдана сфері приватного життя або спричинена внаслідок втрати конфіденційності;*

Коли визначено можливі ризики та їхні джерела. Необхідно обрати конкретні заходи для подальшої мінімізації кожного ризику, наприклад:

- ✓ *внесення змін до політики приватності, враховуючи інтереси суб'єктів, і надання їм якомога конкретнішої інформації (під час розроблення політики приватності і її мовних версій необхідно також зважати на те, чи суб'єкти персональних даних, на права яких впливатиме відеоспостереження, є виключно громадянами України);*
- ✓ *забезпечення суб'єктів персональних даних реальним, швидким і зрозумілим інструментом для реалізації прав, зокрема, отримання інформації щодо впливу на їх приватність, заперечення проти обробки своїх персональних даних і відмови від неї, де це можливо;*
- ✓ *прийняття рішення про відмову від збирання певних категорій даних;*

- ✓ *відмова від підключення комп'ютерної техніки, що використовується для обробки даних, до мережі Інтернет та автоматичного підключення до WI-FI;*
- ✓ *зменшення кута огляду камер, щоб вони охоплювали меншу частину простору/меншу кількість суб'єктів персональних даних;*
- ✓ *прийняття рішення про відмову від використання додаткових технологій, зокрема функції аудіозапису, відеоаналітики (певних видів категоризації даних або поєднання/співвідношення відеозаписів із будь-якими іншими даними, наявними у системі, розпізнавання обличчя тощо);*
- ✓ *відмова від застосування автоматичної обробки персональних даних, що навіть опосередковано може спричинити будь-які правові наслідки для суб'єкта персональних даних або призвести до дискримінації;*
- ✓ *скорочення строків збереження персональних даних, встановлення правил і технологій систематичного автоматичного видалення відеозаписів, аналітичних даних, системних даних, що акумулюються в реєстраційних файлах серверів, тощо;*
- ✓ *вжиття додаткових технічних заходів безпеки (шифрування, обмеження доступу до даних шляхом встановлення ключів, авторизації і автоматичного логування кожного доступу до записів, аналітичних даних і проведених операцій із ними, встановлення захисту від MITM-атак);*

- ✓ *забезпечення навчання персоналу щодо управління ризиками, що можуть впливати на приватність;*
- ✓ *конкретизація угод із розпорядниками і третіми особами, встановлення чітких вимог до обміну персональними даними та їх обробки;*
- ✓ *розроблення внутрішніх правил щодо мінімізації ризиків, що також мають бути частиною обов'язків, покладених на розпорядників і третіх осіб у разі їхнього залучення;*
- ✓ *прийняття рішення про анонімізацію та псевдонімізацію даних;*
- ✓ *прийняття рішення про використання іншої технології, яка є менш інтрузивною;*
- ✓ *будь-які інші заходи, спрямовані на мінімізацію ризиків та збалансування обраних заходів для досягнення визначеної мети з правом суб'єктів персональних даних на невтручання у приватне життя.*

Крок 3. Оцініть необхідну кількість і тип камер, параметри яких будуть пропорційні визначеній меті

Важливе значення для мінімізації ризиків має правильне розташування камер відеоспостереження, тобто встановлення їх таким чином, щоб зображення мало необхідну якість, освітлення і розширення та охоплювало

виключно ту частину простору, що є необхідною і достатньою для досягнення визначеної мети.

Приклад. *Власник відкритого літнього ресторану, розташованого у межах паркової зони, приймає рішення про встановлення систем відеоспостереження з метою підтримання порядку і запобігання крадіжкам у межах ресторану.*

Під час встановлення камер йому необхідно врахувати, що кут огляду камери має обмежуватися виключно територією ресторану і прилеглих приміщень (зон входу/виходу, паркінгу, місць відведених для залишення речей, тощо) без охоплення зон відпочинку у межах парку та сусідніх будівель.

Також власник ресторану має пам'ятати, що кут огляду камер не повинен захоплювати окремі частини ресторану або прилеглі приміщення, в яких суб'єкти мають розумне очікування поваги до приватності (зони вбиралень, ванні кімнати, роздягальні тощо).

Щодо якості зображення відеозапису, то розмір і роздільна здатність кінцевого зображення має важливе значення у контексті дотримання принципу пропорційності.

У разі здійснення відеоспостереження з метою ідентифікації особи необхідно обрати камеру із високою якістю зображення, оскільки використання камер із низькою якістю пропорційно збільшує ймовірність помилкових збігів, що ставить під сумнів досягнення визначеної мети.

Разом із тим, якщо відеоспостереження здійснюється з метою, що не передбачає ідентифікації, а лише, наприклад, виявлення переміщення окремих суб'єктів, сукупності людей або трафіку, встановлення камер із високою роздільною здатністю і можливістю масштабування є надлишковим заходом для досягнення мети, тому у цьому випадку від таких камер варто відмовитись.

Крок 4. Оцініть, чи є необхідним і пропорційним для досягнення мети використання додаткового технічного функціоналу, що є в окремих типах камер

- ***технологія розпізнавання обличчя (ТРО)***

У зв'язку зі швидким розвитком нових технологій і цифровізації більшості сфер життя ТРО (зокрема в режимі реального часу) швидко поширюється у світі.

ТРО – це автоматизована обробка цифрових зображень, що містять людське обличчя, в режимі реального часу з метою ідентифікації, автентифікації, верифікації або категоризації суб'єктів персональних даних. Система побудована на ідентифікації особи через профіль, який зберігається в базі даних у форматі фото та відео.

ТРО є прикладом технології, що обробляє біометричні дані, які статтею 7 Закону України «Про захист персональних даних» віднесено до чутливих даних, щодо обробки яких встановлено особливі вимоги.

Біометричні дані дають змогу точно ідентифікувати людину на основі її біологічних чи поведінкових особливостей, таких, як відбитки пальців, райдужна оболонка ока або риси обличчя. Ці особливості більш постійні, ніж інші персональні дані. Дані про зображення людини можуть бути використані для точної ідентифікації особи в різних контекстах, а також для аналізу або визначення інших характеристик, таких, як вік, стать чи етнічна приналежність.

Таким чином, обробка біометричних даних має здійснюватися на підставі та відповідно до вимог чинного законодавства, що було підтверджено останньою європейською практикою. Загальний регламент про захист даних (GDPR) аналогічно до чинного Закону України «Про захист персональних даних» дозволяє обробку таких даних лише у вийняткових випадках та за умови встановлення відповідних гарантій, адаптованих під ці ризики. Директива про захист даних у зв'язку з правоохоронною діяльністю керується тією самою логікою, дозволяючи обробляти такі дані лише у випадках, коли вони є абсолютно необхідними для досягнення мети.

Приклад. *У лютому 2019 року ТРО було вперше експериментально використано у Франції з правоохоронною метою під час карнавалу у місті Ніцца. Це викликало багато дискусій щодо впливу технології на приватність, зокрема у поєднанні з існуючими у Франції автоматизованими прикордонними пунктами пропуску «PARAFE», які працюють на основі ТРО та автоматично ідентифікують суб'єктів персональних даних шляхом порівняння інформації, зчитаної з паспорта, з інформацією, отриманою за результатами розпізнавання обличчя суб'єкта в режимі реального часу.*

Використання технології у Ніцці було схвалено французьким регулятором у сфері захисту персональних даних (CNIL). Разом із тим не всі експериментальні проекти, за результатами аналізу CNIL, визнані такими, що відповідають вимогам законодавства

про захист персональних даних. Наприклад, проєкт, що передбачав сканування обличчя у середніх школах, не було схвалено французьким регулятором через невідповідність Загальному регламенту про захист даних.

- ***розпізнавання номерних знаків автомобілів***

Згідно з чинним Законом України «Про захист персональних даних» персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Зважаючи на незворотність євроінтеграційного курсу України, закріпленого на рівні Конституції, наразі триває реформування законодавчого регулювання сфери захисту персональних даних з метою приведення національного законодавства у відповідність до кращих європейських стандартів захисту права на приватність.

У Верховній Раді України зареєстровано новий проєкт закону «Про захист персональних даних», розроблений із урахуванням вимог до захисту персональних даних, відображених у Загальному регламенті про захист даних, з метою імплементації його положень в українське законодавство.

Загальний регламент про захист даних визначає персональні дані як будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати. При цьому визначається, що фізична особа, яку можна ідентифікувати, є такою, що може бути ідентифікована прямо або опосередковано, зокрема, за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

Ураховуючи кращий європейський досвід, перед прийняттям рішення про застосування технології розпізнавання номерних знаків автомобілів варто усвідомлювати, що це дані, які дають змогу опосередковано здійснити ідентифікацію особи. Це означає, що такі дані у поєднанні з іншою інформацією або технологією (наприклад, розпізнавання обличчя) можуть ідентифікувати особу і сформувати профіль щодо її поведінки, переміщення і приватного життя загалом.

Отже, під час прийняття рішення про використання такої технології необхідно враховувати наявність законної підстави, мету встановлення відеоспостереження, специфічні ризики, які ця технологія може мати для

права на приватність, і у разі прийняття рішення про її використання розробити відповідні заходи для мінімізації таких ризиків.

- ***аудіофіксація***

З огляду на те, що сьогодні існує велика кількість камер із можливістю аудіофіксації, під час вибору типу камери для майбутнього відеоспостереження необхідно визначити, чи існує законна підстава для обробки аудіофайлів, які містять, зокрема дані про голос окремих суб'єктів та про предмет їхніх приватних розмов у публічних місцях, і оцінити чи є обробка таких даних необхідним і пропорційним заходом для досягнення визначеної мети, належним чином обґрунтувавши це.

У разі відсутності законних підстав для обробки аудіофайлів та у разі якщо визначеної мети можна досягти менш інтрузивним шляхом варто відмовитись від використання камер, що містять функцію аудіозапису.

- ***безпілотний літальний апарат (дрон)***

На сьогодні дрони активно використовуються для різних цілей, зокрема: особистих побутових цілей; правоохоронних цілей; професійних і комерційних, наприклад, для моніторингу безпеки приміщень, моніторингу важкодоступних об'єктів інфраструктури, моніторингу стану приміщень та оцінки збитків.

Однак необхідно усвідомлювати, що використання дронів може залишатися непомітними протягом тривалого часу і водночас збирати багато персональних даних, у тому числі й чутливих.

Європейському досвіду у цій сфері притаманне застосування різних підходів до використання дронів (та відеоспостереження загалом) в залежності від цілей (особисті побутові/професійні або комерційні потреби). Зокрема, у разі застосування дронів для відеоспостереження у цілях відмінних від побутових володільці зобов'язані забезпечити відповідність застосування дронів чинним вимогам законодавства у сфері захисту персональних даних.

Мобільність дрона може спричинити обмеження низки прав суб'єктів персональних даних. Зокрема, позбавити їх можливості безперешкодно отримати інформацію щодо здійснення такого відеоспостереження.

При цьому в статті 8 Конвенції про захист прав людини і основоположних свобод, яка ратифікована і є частиною національного законодавства України, передбачено, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Водночас органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Відтак при прийнятті рішення щодо використання дрона для здійснення відеоспостереження з визначеною попередньо метою володільцю важливо враховувати:

- ✓ *наявність законної підстави для його застосування;*
- ✓ *дотримання принципу пропорційності та збалансованості прав, який означає, що будь-які обмежувальні заходи мають відповідати сутності основних прав і свобод та бути необхідними заходами у демократичному суспільстві.*

Отже, ті чи інші заходи, що передбачають обмеження прав, вживаються виключно за умови доведеності їх потенційної переваги для цілей суспільства над тими засобами, які передбачають менше втручання в особисте життя.

У разі ж прийняття рішення про використання дрона для здійснення відеоспостереження володільцю необхідно вжити всіх можливих організаційних і технічних заходів для забезпечення прав суб'єктів персональних даних та мінімізації ризиків.

Приклад. *Власник телекомунікаційної компанії прийняв рішення про використання дрона з метою зйомки рекламного ролика.*

Для належного повідомлення щодо здійснення відеозапису за допомогою дрона власник передбачив спеціальну форму одягу для особи, що керуватиме дроном, яка є помітною, і сигналізуватиме про те, ким здійснюється відеоспостереження, та дає можливість суб'єкту персональних даних звернутися за деталізованою інформацією.

Також у межах простору, який потрапляє до камери, за кілька днів до зйомки розташовано тимчасові мобільні попереджувальні знаки/постери.

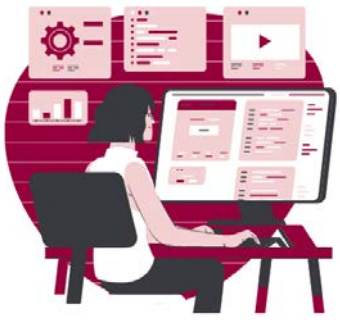
<u>Крок 5.</u> Оцініть необхідні строки зберігання записів відповідно до цілей та розробіть правила їх систематичного видалення

З метою запобігання можливим порушенням права на приватність до прийняття рішення про встановлення систем відеоспостереження необхідно передбачити дотримання принципу обмеженого зберігання даних, який полягає в тому, що персональні дані можуть зберігатися у формі, що дає можливість ідентифікувати суб'єктів, не довше, ніж це необхідно для досягнення визначеної мети.

У деяких випадках персональні дані можуть зберігатися протягом більш тривалих періодів, проте лише доти, доки вони опрацьовуються винятково для досягнення значного суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей, і за умов вжиття відповідних технічних та організаційних заходів задля гарантування прав і свобод суб'єкта даних.

Дотримання принципу обмеженого зберігання даних може бути забезпечено шляхом встановлення чітких правил видалення відеозаписів і пов'язаних із ними даних за певним розкладом.

Тому до прийняття рішення про встановлення систем відеоспостереження володільцю необхідно попередньо визначити строки зберігання та розклад видалення даних і як буде організовано ці процеси.



Видалення можна забезпечити як автоматично, так і за допомогою уповноважених працівників, яким надано необхідний рівень доступу до даних, або за допомогою використання камер із можливістю здійснення циклічного запису, тобто систематичного автоматичного перезапису матеріалу на один і той самий носій.

Приклад. *Під час проведеної Офісом Інформаційного Комісара Сполученого Королівства перевірки було виявлено, що Поліція Південного Уельсу зберігала здійснені відеозаписи протягом 31 дня, а Управління поліції Лондона – протягом 30 днів. При цьому обидві служби поліції видаляли записи, здійснені з використанням технології розпізнавання обличчя, після їх обробки відповідно до встановленої мети, якщо не було сигналу тривоги або збігу.*

Закон про захист даних Сполученого Королівства (DPA 2018) не встановлює конкретних графіків збереження для окремих типів даних, однак усі підрозділи поліції

Сполученого Королівства підпорядковуються національним критеріям оцінки зберігання та стандартам управління інформацією правоохоронних органів.

Зокрема, кожен підрозділ поліції, що використовує технологію розпізнавання обличчя, має встановлювати графіки зберігання/видалення даних відповідно до законодавчих вимог як частину системи оцінки впливу на захист даних. (https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf)

Крок 6. Визначте майбутнє місце зберігання відеозаписів

Персональні дані мають оброблятись у спосіб, що забезпечує належну їх безпеку, зокрема, шляхом захисту проти несанкціонованої чи незаконної обробки та проти ненавмисної втрати, знищення чи завдання шкоди, із застосуванням відповідних технічних і організаційних інструментів.

Таким чином, технічне обладнання призначене для зберігання та аналізу відеозаписів (серверні, ситуаційні центри) має зберігатися в окремому приміщенні, доступ до якого має бути обмеженим і контрольованим.

При цьому рекомендовано до прийняття рішення про встановлення систем відеоспостереження передбачити як здійснюватиметься навчання працівників щодо забезпечення належної і коректної роботи зазначених систем та дотримання встановлених правил роботи із персональними даними.

РОЗДІЛ ІІ. ДІЇ, ЩО НЕОБХІДНО ЗДІЙСНИТИ ПІСЛЯ ПРИЙНЯТТЯ РІШЕННЯ ПРО ВСТАНОВЛЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Крок 1. Розмістіть повідомлення суб'єктів персональних даних про здійснення відеоспостереження

Суб'єкт персональних даних має право заздалегідь знати про те, що у зоні його перебування здійснюється відеоспостереження, мати доступ до інформації про те, ким і з якою метою воно здійснюється, який порядок обробки персональних даних із використанням систем відеоспостереження, а також має право переглянути записи або звернутись із запитом про отримання копій відеозаписів за його участі.

Тому після прийняття рішення про встановлення систем відеоспостереження необхідно розмістити у межах простору, де воно здійснюється, достатньо помітне і зрозуміле повідомлення. Таке повідомлення має містити інформацію про те, хто і з якою метою здійснює відеоспостереження, контакти відповідальної особи, інформацію про використання специфічного технічного функціоналу камери (у разі використання), а також посилання на більш детальну інформацію щодо порядку здійснення відеоспостереження та обробки персональних даних.

При цьому повідомлення про здійснення відеоспостереження має бути розміщене в такому форматі, щоб це було першим, що помічає суб'єкт персональних даних, коли потрапляє в зону здійснення відеоспостереження. Ця рекомендація стосується всіх видів відеоспостереження, встановлюваних у межах територій, що перебувають у постійному або тимчасовому загальному користуванні суспільства.

Після прийняття рішення про встановлення систем відеоспостереження також рекомендується вжити заходів щодо навчання працівників, відповідальних осіб і забезпечення їх необхідними інструкціями/алгоритмами дій для надання відповідної реакції у разі звернення суб'єкта персональних даних за додатковою інформацією щодо здійснюваного відеоспостереження або із запитом про отримання копій відеозаписів.

Приклад. *Власниця готельного комплексу із рестораном прийняла рішення про встановлення систем відеоспостереження з метою підтримання порядку і запобігання крадіжкам.*

Для належного інформування гостей про здійснення відеоспостереження на всіх входах до комплексу і в кожному приміщенні було встановлено відповідні таблички і плакати, а також відповідні мініатюри повідомлення було включено до Правил проживання в готелі та Меню ресторану.

Крок 2. Розробіть внутрішні документи, які будуть врегульовувати усі процеси обробки персональних даних

Заходи, спрямовані на безпеку обробки персональних даних, та процедури обробки, можуть відображатися в одному або кількох окремих документах, наприклад, порядку обробки персональних даних та порядку здійснення відеоспостереження. Такі документи можуть бути оформлені у довільній формі.

Перелік конкретних заходів і документів залежить від специфіки діяльності володільця/розпорядника, набору функцій відеокамер та інформаційних систем, кількості персоналу, залученого до роботи з даними тощо.

З метою належного захисту персональних даних рекомендується орієнтуватися на таке наповнення документації:

Загальні положення:

- ✓ *законна підстава та мета обробки даних;*
- ✓ *обсяг та категорії даних у співвідношенні з конкретними цілями їх обробки;*
- ✓ *основні принципи, якими керується володілець та уповноважені ним особи під час обробки даних.*

Права суб'єкта персональних даних:

- ✓ *право на інформування;*
- ✓ *право на доступ до своїх персональних даних;*
- ✓ *право на виправлення та видалення своїх персональних даних;*
- ✓ *право на заперечення проти обробки своїх персональних даних;*
- ✓ *процедура розгляду запитів та оскарження.*

Процедури обробки персональних даних:

- ✓ *інформаційні системи, програмне забезпечення, сервери, задіяні у процесі обробки персональних даних;*
- ✓ *перелік організаційних та технічних заходів безпеки;*
- ✓ *строк зберігання та порядок видалення інформації.*

Обробка даних, що здійснюється розпорядниками:

- ✓ *загальні положення про умови та мету передачі персональних даних;*
- ✓ *правила виконання вимог щодо захисту персональних даних;*
- ✓ *заходи у разі припинення договірних відносин.*

Передача персональних даних третім особам:

- ✓ *процедури та правила передачі персональних даних третім особам;*
- ✓ *порядок здійснення контролю.*

Внутрішній контроль:

- ✓ *особа, відповідальна за безпеку персональних даних;*
- ✓ *порядок надання права доступу працівників до персональних даних;*
- ✓ *проведення внутрішніх перевірок щодо дотримання правил безпеки при обробці персональних даних.*

З метою забезпечення принципів «прозорості» і «підзвітності», документи щодо обробки персональних даних мають бути у вільному доступі.

Це може бути реалізовано шляхом оприлюднення документації на офіційному сайті володільця/розпорядника, розміщення штрих-коду/посилання у відповідних повідомленнях про здійснення відеоспостереження або забезпечити доступність для ознайомлення в інший спосіб.

Крок 3. Розробіть внутрішні правила доступу до персональних даних

Доступ до систем відеоспостереження, записів, серверів та аналітичних даних, пов'язаних із відеоспостереженням, має бути обмеженим. Тому після прийняття рішення про встановлення систем відеоспостереження рекомендується чітко визначити коло осіб, що матимуть доступ до цієї інформації, та покласти на них відповідальність за захист персональних даних.

Варто також звернути увагу на те, що різні працівники можуть мати різний рівень доступу до інформації. Будь-яке надання, зміна або анулювання прав доступу має здійснюватися відповідно до критеріїв, визначених у внутрішніх документах.

Приклад. *Особи, які працюють з системами відеоспостереження, можуть мати різні посадові обов'язки, наприклад, технічне обслуговування або моніторинг зображень. Тому вони повинні мати й різні права доступу.*

При цьому один користувач системи відеоспостереження матиме доступ до збереження, копіювання або видалення записаного матеріалу за встановленими правилами та розкладом, тоді як інший матиме право лише переглядати записи.

До організаційних заходів безпеки обробки персональних даних також рекомендується обов'язково включати систематичне навчання працівників, що мають права доступу або працюють з персональними даними.

Працівники мають добре розумітися на внутрішніх правилах, зокрема щодо строків зберігання даних, порядку їх видалення, недопущення розголошення персональних даних, до яких їм надано доступ або які стали їм відомі у зв'язку з виконанням професійних (або службових) обов'язків тощо.

Приклад. *Неприпустимо, щоб відеозапис, який здійснено з метою запобігання та оперативного реагування на правопорушення, був поширений у соціальних мережах для демонстрації курйозних випадків за участі суб'єктів персональних даних, якщо при цьому вони прямо чи опосередковано можуть бути ідентифіковані на цьому відео.*

Крок 4. Розробіть правила надання доступу до персональних даних для третіх осіб

Вимоги до надання доступу до персональних даних третім особам визначено в частинах 1-5 статті 16 та частинах 2-3 статті 17 Закону України «Про захист персональних даних».

Тому під час розробки правил надання доступу кожен володілець має враховувати визначені законодавством вимоги, а також у кожному індивідуальному випадку самостійно оцінювати спроможність третьої особи забезпечити виконання вимог законодавства у сфері захисту персональних даних.

З цією метою під час вирішення питання про надання доступу варто здійснювати ретельну оцінку правових підстав для запиту, повноважень запитувача, а також пропорційності обсягу запитуваних даних переслідуваній меті.

Приклад. *Для правоохоронних органів належною підставою для отримання доступу до даних в рамках кримінального провадження є ухвала слідчого судді, суду про тимчасовий доступ до речей і документів.*

Крок 5. Забезпечте ведення реєстру обробки персональних даних

Для належного захисту права на захист персональних даних і запобігання будь-яким порушенням, зокрема внаслідок несанкціонованого доступу, рекомендується вести реєстр усіх дій, що вчиняються із персональними даними.

Такий реєстр може містити щонайменше:

- ✓ *інформацію про розташування камери, дату й час запису;*
- ✓ *найменування та/або посаду особи, що здійснює обробку даних;*
- ✓ *інформацію про рівень доступу особи до даних;*
- ✓ *інформацію про проходження/непроходження авторизації, застосування ключів;*
- ✓ *інформацію про дію (перегляд, передача, архівування, видалення тощо).*

У разі надання доступу до персональних даних третім особам:

- ✓ *найменування організації/установи та/або посаду особи, що запитує інформацію;*
- ✓ *обсяг запитуваних даних;*
- ✓ *повноваження, мету, підстави для запиту;*
- ✓ *дату, час і спосіб надання інформації;*
- ✓ *аргументацію щодо прийнятого рішення (про надання/відмову);*
- ✓ *інформацію про особу, що надала доступ.*

Крок 6. Призначте відповідальну особу або створіть підрозділ, що відповідатиме за захист персональних даних

Згідно з частиною другою статті 24 Закону України «Про захист персональних даних» органи державної влади, органи місцевого самоврядування, а також володільці чи розпорядники персональних даних, що здійснюють обробку персональних даних, створюють (визначають) структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних під час їх обробки.

При цьому фізичні особи - підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати та нотаріуси особисто забезпечують захист персональних даних згідно з вимогами чинного законодавства.

Структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних, а також взаємодіє з Уповноваженим та визначеними ним посадовими особами з питань запобігання та усунення порушень законодавства про захист персональних даних.

Факт створення нового підрозділу, покладення нових обов’язків на відповідальну особу і перелік таких обов’язків рекомендується закріпити у внутрішніх документах.

Серед обов’язків відповідальної особи доцільно визначити:

- ✓ *здійснення внутрішнього контролю за дотриманням законодавства про захист персональних даних;*
- ✓ *здійснення внутрішнього контролю за вжиттям заходів, спрямованих на безпеку обробки персональних даних;*
- ✓ *ведення реєстру обробки персональних даних;*
- ✓ *актуалізація внутрішньої документації з питань захисту персональних даних;*
- ✓ *навчання працівників;*
- ✓ *організацію розгляду запитів суб'єктів персональних даних та третіх осіб;*
- ✓ *підготовку до перевірок органами контролю.*

Крок 7. Забезпечте необхідний рівень безпеки обробки персональних даних

Володілець та розпорядник самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки, з урахуванням вимог законодавства у сферах захисту персональних даних та інформаційної безпеки.

Організаційні заходи можуть охоплювати, зокрема:

- ✓ *визначення порядку доступу до персональних даних працівників володільця/розпорядника;*
- ✓ *визначення порядку ведення обліку операцій, пов’язаних з обробкою персональних даних суб’єкта та доступом до них;*
- ✓ *розроблення плану дій у разі несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;*
- ✓ *систематичне навчання співробітників, які працюють з персональними даними;*

- ✓ *розташування моніторів для перегляду відеозаписів з камер таким чином, щоб унеможливити несанкціонований перегляд;*
- ✓ *попередження працівників про обережну роботу з електронними листами, зокрема тими, в яких пропонується перейти за посиланням на інший сайт, тощо.*

Технічні заходи можуть включати:

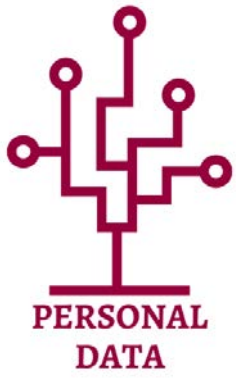
- ✓ *застосування двофазної автентифікації (наприклад, поєднання пароля із ключем/PIN-кодом);*
- ✓ *використання надійних ключів для шифрування/розшифрування інформації;*
- ✓ *відмова від автоматичного підключення до Wi-Fi-мереж;*
- ✓ *встановлення процедур автоматичного логування доступу до записів, аналітичних даних;*
- ✓ *реєстрацію здійснених операцій із ними; встановлення антивірусного програмного забезпечення тощо.*

Також рекомендується постійно оцінювати ефективність заходів, спрямованих на безпеку персональних даних, і оновлювати їх відповідно до будь-яких змін.

РОЗДІЛ ІІІ. ДІЇ, ЩО НЕОБХІДНО ЗДІЙСНИТИ, ЯКЩО ВІДБУВСЯ ВИТІК ІНФОРМАЦІЇ

З урахуванням чинного законодавства України та кращих європейських практик рекомендується до плану дій володільця/розпорядника у разі несанкціонованого доступу до персональних даних включати наступні кроки.

Крок 1. Перевірте, чи є персональні дані частиною інформації, що стала предметом витоку



Передусім необхідно визначити, яка саме інформація була поширена і чи може вона самостійно або в поєднанні з іншими даними, що знаходяться у відкритому доступі, призвести до ідентифікації осіб або завдати будь-якої іншої шкоди сфері приватного життя чи іншій сфері життя внаслідок втрати конфіденційності.

У зв'язку з цим доцільно мати актуалізовані документи (порядок здійснення відеоспостереження, порядок обробки персональних даних, політика приватності тощо), де викладено максимально повний перелік персональних даних, які обробляються володільцем та/або розпорядником (не лише у зв'язку із застосуванням відеоспостереження).

Також потрібно визначити, які саме категорії персональних даних стали предметом витоку. Від цього залежить рівень потенційного ризику для права на приватність і подальші заходи, спрямовані на припинення порушення.

Приклад. *Через помилку в адресі електронної розсилки було поширено чутливі дані. Такий витік становитиме вищий рівень загрози для приватності і впливатиме на інші фундаментальні права суб'єкта персональних даних, аніж якщо було б поширено дані про його/її вік.*

Крок 2. Оцініть коло суб'єктів, що отримали несанкціонований доступ до персональних даних

З метою ефективного визначення подальших заходів для мінімізації шкоди правам суб'єктів, оцінка ризиків має бути якомога повною. Тому після визначення категорій поширених персональних даних необхідно також

визначити категорії суб'єктів, що отримали несанкціонований доступ до персональних даних, і співвіднести їх із категоріями даних, що стали предметом витоку. Чим ширшим є коло суб'єктів, тим вищим є ризик.

Приклад. *Під час надання відповіді на запит суб'єкта персональних даних про отримання копій відеозаписів за його участю, здійснених на терасі ресторану, було допущено помилку в стрічці адресата, і відеозаписи разом із ПІБ і контактними даними суб'єкта було надіслано на робочі адреси деяких працівників володільця, які згідно з порядком обробки персональних даних не мали доступу до цих даних.*

У цьому випадку коло осіб, що випадково отримали несанкціонований доступ до зазначених даних, є вузьким, конкретним і становить менший ризик, ніж якщо б сукупність зазначених даних було поширено на сторонні зовнішні адреси або на адреси інших клієнтів закладу. Такий виток можна взяти під контроль і мінімізувати шкоду.

У разі поширення даних на сторонні зовнішні адреси або на адреси інших клієнтів закладу ризик заподіяної або потенційної шкоди приватності значно зростає.

Крок 3. Оцініть коло суб'єктів, чиє право на приватність може бути порушене внаслідок витоку

Оцінювання ризику також має містити заходи щодо визначення якомога чіткішого обсягу шкоди, якої суб'єкти персональних даних потенційно можуть зазнати від витоку персональних даних.

Для цього пропонується визначити:

- ✓ *кількість суб'єктів персональних даних, чиї дані стали предметом витоку;*
- ✓ *чи є серед цих суб'єктів діти або інші вразливі категорії населення;*
- ✓ *чи становить такий виток ризик небезпеки для життя або майна для когось із суб'єктів персональних даних;*
- ✓ *чи можуть незаконно поширені персональні дані бути надалі використані зі злочинним наміром;*
- ✓ *яких технічних чи організаційних заходів необхідно негайно вжити для відновлення права на приватність.*

Крок 4. Забезпечте негайне вжиття організаційних і технічних заходів, спрямованих на припинення порушення та відновлення захисту даних

Внаслідок незаконного поширення персональних даних володілець/розпорядник зазвичай стикається із фінансовими та

репутаційними ризиками. Проте, зважаючи на специфіку права на приватність, що тісно пов'язане і впливає на інші фундаментальні права, мінімізація ризиків для суб'єктів персональних даних має бути пріоритетом для володільця/розпорядника.

Після того, як було визначено:

- ✓ *які персональні дані поширено;*
- ✓ *які категорії суб'єктів потенційно чи реально перебувають під загрозою;*
- ✓ *коло осіб, що отримали несанкціонований доступ до персональних даних;*
- ✓ *обсяг завданої чи потенційної шкоди для права на приватність та інших прав суб'єктів персональних даних;*

необхідно самостійно обрати організаційні та технічні заходи для мінімізації шкоди правам/їх відновлення.

Приклади. *У разі виникнення підозри про можливий витік персональних даних і несанкціонований доступ до них у зв'язку з викраденням/втратою корпоративного технічного обладнання та електронних носіїв, одним із заходів, спрямованих на мінімізацію ризиків, може бути, наприклад, зміна паролів або віддалене видалення інформації або будь-які інші доступні на момент інциденту технічні інструменти.*

У разі допущення помилки в електронній адресі і надсиланні персональних даних стороннім особам, що не уповноважені мати доступ до цих даних, можна невідкладно надіслати запит про видалення попереднього листа, уникаючи відкриття вкладень, або організувати внутрішній та зовнішній обмін інформацією, що містить персональні дані, виключно із використанням ключів для доступу до зашифрованого вмісту тих чи інших файлів. Тобто так, щоб відкрити файл з інформацією про себе міг лише конкретний суб'єкт персональних даних, якому належать ці персональні дані, або уповноважена на це особа.

У разі, якщо ризик залишається і потенційно впливає на інші права, необхідно негайно повідомити суб'єкта персональних даних про випадок несанкціонованого доступу третіх осіб до його персональних даних.

У разі виникнення труднощів із самостійним визначенням необхідних організаційних заходів для мінімізації шкоди і відновлення права на приватність рекомендується звернутись за додатковими роз'ясненнями щодо кожної окремої ситуації до Уповноваженого Верховної Ради України з прав людини.

Варто нагадати, що відповідно до статті 27 Закону України «Про захист персональних даних» професійні, самоврядні та інші громадські об’єднання чи юридичні особи можуть розробляти кодекси поведінки з метою забезпечення ефективного захисту прав суб’єктів персональних даних, додержання законодавства про захист персональних даних з урахуванням специфіки обробки персональних даних у різних сферах.

При розробленні такого кодексу поведінки або внесенні змін до нього відповідне об’єднання чи юридична особа може звернутися за висновком до Уповноваженого Верховної Ради України з прав людини.