



**РОЗ'ЯСНЕННЯ
УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ
З ПРАВ ЛЮДИНИ**

**«КАМЕРИ ВІДЕОСПОСТЕРЕЖЕННЯ: ЩО ВАРТО ЗНАТИ
КОЖНОМУ, ЩОБ ЗАХИСТИТИ СВОЮ ПРИВАТНІСТЬ?»**

Київ
2022

Рекомендації розроблено за участю:

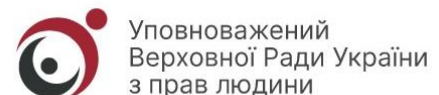
Інни Берназюк, представника Уповноваженого у сфері захисту персональних даних

Олени Гунько, завідувача сектору упровадження міжнародних стандартів у сфері захисту персональних даних Департаменту у сфері захисту персональних даних Секретаріату Уповноваженого

Уляни Шадської, експерта Проекту «EU4DigitalUA»

Цільова аудиторія: громадяни України, іноземці та особи без громадянства, що проживають на території України.

Дизайн створено з використанням платформи графічного дизайну Canva.



EU4DigitalUA project is part of the European Union's support to Ukraine. The views, thoughts, opinions and conclusions expressed in the text belong solely to the author, and not necessarily represent the position of the project, European Union or FIIAPP.

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ I. ВІДЕОПОСТЕРЕЖЕННЯ В МАГАЗИНАХ, РЕСТОРАНАХ ТА ТОРГОВЕЛЬНО-РОЗВАЖАЛЬНИХ ЦЕНТРАХ.....	6
РОЗДІЛ II. ВІДЕОПОСТЕРЕЖЕННЯ В РАМКАХ ТРУДОВИХ ВІДНОСИН.....	12
РОЗДІЛ III. ВІДЕОПОСТЕРЕЖЕННЯ В БАГАТОПОВЕРХОВИХ БУДИНКАХ ТА НА ТЕРИТОРІЇ ЖИТЛОВИХ КОМПЛЕКСІВ.....	18
РОЗДІЛ IV. КАМЕРИ ВІДЕОФІКСАЦІЇ НА ДОРОГАХ ТА В ГРОМАДСЬКОМУ ТРАНСПОРТІ.....	23

ВСТУП

Системи відеоспостереження стали важливим атрибутом інфраструктури міст і селищ. Відеокамери встановлюються всередині багатоповерхових будинків, на території житлових комплексів, у магазинах і торговельних центрах, на дорогах та транспортних магістралях. Також використовуються мобільні відеокамери як частини безпілотних літальних апаратів (дронів). Розвиток технологій відеоспостереження викликає багато запитань у суспільства щодо того, чи не порушує це їхнього права на приватність, зокрема в частині захисту персональних даних.

Чи збираються персональні дані за допомогою відеокамер?

Так. За допомогою відеозапису можна ідентифікувати особу за різними її ознаками — рисами обличчя, параметрами тіла, голосу, особливостями поведінки тощо. Такі дані дають змогу точно впізнати людину через її фізіологічні чи поведінкові особливості.

Відеокамери, встановлені у громадських місцях, дають можливість зафіксувати місцезнаходження/перебування людини у певних закладах (зокрема, медичних або релігійних), на мирних зібраннях під час висловлення своїх переконань. Також завдяки використанню систем відеоспостереження (камер, поєднаних в одну мережу) можна дізнатися маршрути пересування людини містом, її побутові звички та інші подробиці особистого чи професійного життя.

Таким чином, здійснення відеоспостереження незалежно від того, чи зберігаються записи, є обробкою персональних даних і регулюється законодавством про захист персональних даних.

Чи становлять загрозу відеокамери?

Новітні технології мають позитивний вплив: допомагають покращити роботу органів правопорядку або рятувальних служб. Наприклад, дають змогу швидко розкрити злочин, надати першу допомогу чи навіть відреагувати на стихійне лихо.

Водночас існує низка ризиків, які суспільство має усвідомлювати й мати змогу захистити себе. Зокрема, коли відеоспостереження здійснюється з незаконною метою, збирається більше персональних даних, ніж це необхідно, або якщо доступ до відеозаписів отримують сторонні особи. Відеозаписи можуть використовувати для переслідування людей у зв'язку з їхньою професійною діяльністю або переконаннями.

Також системи відеоспостереження можна пошкодити. У різних країнах світу вже зафіксовано непоодинокі випадки¹, коли хакери² підключаються до камер і отримують інформацію, щоб шантажувати людей. У 2020 році було проведено дослідження³, у резуль-

¹Наприклад, The Guardian повідомляє про десятки людей, які подали позов до суду на компанію Ring після того, як хакери приєдналися до домашніх камер Ring, будили людей серед ночі, розмовляли з дітьми, коментували події в спальні, погрожували, шантажували й ображали.

²Особи, що намагаються отримати несанкціонований доступ до комп'ютерних систем з метою отримання секретної (конфіденційної) інформації.

³[https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/65154/Tyson Your Privilege Gives 2020 Accepted.pdf](https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/65154/Tyson%20Your%20Privilege%20Gives%202020%20Accepted.pdf)

таті якого команда вчених дійшла висновку, що зловмисники можуть шпигувати за допомогою домашніх камер відеоспостереження. Це означає, що така ситуація може статися і з системами, які встановлюють у громадських місцях.

Про що цей документ?

З огляду на те, що популярність відеоспостереження і надалі зростає, а з цим зростає й кількість ризиків втручання у приватне життя осіб, Уповноваженим Верховної Ради України з прав людини розроблено це роз'яснення у формі запитань-відповідей зі спрощеною термінологією, щоб кожна людина могла зрозуміти цілі використання таких технологій, а також пов'язані з ними ризики та реалізувати своє право на приватність під час використання систем відеоспостереження.

I. ВІДЕОСПОСТЕРЕЖЕННЯ В МАГАЗИНАХ, РЕСТОРАНАХ ТА ТОРГОВЕЛЬНО-РОЗВАЖАЛЬНИХ ЦЕНТРАХ



Відеоспостереження стало частиною системи безпеки в магазинах, ресторанах і торговельно-розважальних центрах. Камери встановлюються на вході/виході в торговельні зали, у розвантажувальних й касових зонах або складах. Запис може здійснюватися цілодобово або в робочий час, безперервно або реагувати на рух.

Для чого встановлюються відеокамери?

У більшості випадків відеокамери встановлюють для запобігання крадіжкам або псування товарів. Доволі часто відеоспостереження має превентивну функцію — допомагає вчасно втрутитися у конфліктні ситуації та з'ясувати обставини.

Відеокамери часто використовують для контролю не лише за відвідувачами, а й за працівниками. Такі дії потребують від власників магазинів, ресторанів і торговельних центрів встановлення балансу між правом людини на повагу до приватного життя та правом закладу забезпечувати порядок на своїй території. Питання щодо відеоспостереження за працівниками буде детальніше розглянуто у наступному розділі.

Чи збирають відеокамери персональні дані?

Так. Обсяг інформації залежатиме від функціональних можливостей пристроїв. Наприклад, деякі системи оснащені функціями розпізнавання обличчя, аудіозапису або відеоаналітики, тобто отримують можливість розпізнавати відвідувачів за рисами обличчя, голосом, віком, статтю, етнічною приналежністю тощо. Такі функції можуть бути реалізовані завдяки спеціальному програмному забезпеченню та здійснюватися майже на будь-якому відеозаписі.

Чи є правові підстави для встановлення відеокамер?

У законодавстві України, що регулює захист персональних даних, немає заборони встановлювати відеоспостереження на фасаді або в торговому залі магазинів чи інших закладів. Переважно це обґрунтовують як спосіб захисту своїх законних інтересів (тобто забезпечення правопорядку на території закладу, збереження майна тощо).

Разом із тим у Законі України «Про захист персональних даних» визначено, що така правова підстава не застосовується, якщо потреби захисту прав і свобод людини у зв'язку з обробкою її даних буде переважати такі інтереси власника закладу⁴. Тому ця норма закону зобов'язує знаходити баланс між правом особи на приватність та бажанням закладу встановлювати різні технології відеоконтролю.

⁴ Стаття 11 Закону України «Про захист персональних даних».

Також є правила й обмеження щодо збору та використання даних за допомогою пристроїв із можливістю розпізнавання обличчя (face recognition) або інших технологій з використанням алгоритмів штучного інтелекту. Важливо пам'ятати, що особа як суб'єкт персональних даних має право знати про механізм застосування автоматичної обробки своїх даних та захистити свої права, якщо автоматизоване рішення матиме для неї правові наслідки⁵.

Наприклад, коли за допомогою системи відеоспостереження збираються дані та аналізуються для профілювання людей (за віком, статтю, які покупки роблять найчастіше, час відвідування магазину тощо) з маркетинговою метою.

Які існують основні правила й обмеження?



✓ Передусім, відеоспостереження не може бути прихованим⁶. Це означає, що при вході в торговельний зал або ресторан чи всередині приміщення має бути встановлено таблички з повідомленням про здійснення відеоспостереження. Вдалою вважається практика, коли таке оголошення продубльовано іноземною мовою (наприклад англійською), щоб попередити туристів. Людина має право знати про те, хто і з якою метою здійснює відеоспостереження, контакти відповідальної особи, про технічні можливості камери (наприклад запис звуку) та іншу інформацію щодо порядку обробки персональних даних за допомогою відеоспостереження.

✓ Власники закладів мають вжити заходів, спрямованих на захист персональних даних та інформаційної безпеки в цілому. Серед іншого, мають бути розроблені документи, що регулюють процес обробки та захисту такої інформації. Документ може мати назву «Політика приватності», «Політика конфіденційності», «Порядок обробки персональних даних», «Інструкція з обробки персональних даних», «Положення про обробку персональних даних» тощо.

✓ Кут огляду камери повинен обмежуватися виключно територією громадського закладу й прилеглих до нього приміщень (зон входу/виходу, паркінгу, місць, відведених для залишення речей, тощо) без охоплення приватних будинків або так званих режимних об'єктів⁷ (наприклад, наукові лабораторії, що мають оборонне значення, дислокації військових частин тощо).

Де заборонено встановлювати камери?

Заборонено встановлювати камери в туалетних кімнатах, душових, роздягальнях для персоналу, примірочних кабінах та інших місцях, де людина може розраховувати на приватність.

⁵ Стаття 8 Закону України «Про захист персональних даних».

⁶ Для прихованого відеоспостереження використовують спеціальні технічні засоби, які можуть бути непомітні для ока людини. За незаконне отримання інформації за допомогою негласних технічних засобів передбачена кримінальна відповідальність (стаття 359 Кримінального кодексу України «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»).

⁷ У законодавстві немає поняття «режимного об'єкта». Воно є суто розмовним й означає об'єкти, які є особливо важливими для безпеки держави, тобто для них діють спеціальні режими охорони. Служба безпеки України сформувала Звод відомостей, що становлять державну таємницю, де визначено перелік об'єктів, зйомка яких заборонена.

Розміщення відеокамер у їдальнях або загальних зонах відпочинку не заборонено, але потребує розгляду питання щодо необхідності таких заходів для досягнення законної мети (тобто, застосування принципу пропорційності).



Які у вас є права щодо здійснення відеоспостереження?

Передусім ви маєте право⁸:

- знати назву (найменування) та місцезнаходження суб'єкта, що здійснює відеоспостереження;
- знати про законні підстави та джерела збирання даних (розташування камер);
- знати про місцезнаходження своїх персональних даних (де знаходяться відеозаписи) та мету їх обробки;
- знати про умови надання доступу до своїх даних, зокрема інформацію про третіх осіб, яким вони передаються;
- отримувати не пізніш ніж за 30 календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються ваші персональні дані, а також отримувати зміст таких персональних даних;
- пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням;
- право на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- знати механізм автоматизованої обробки персональних даних та мати захист від автоматизованого рішення, яке має для нього правові наслідки;
- отримувати інформацію про умови безпеки та обробки даних;
- отримувати інформацію про свої права та процедуру оскарження, у разі порушення;
- отримувати контактну інформацію, до кого у магазині/ресторані/торговельному центрі можна звернутися з додатковими питаннями у даній сфері;
- звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або суду.

Інформування про відеоспостереження може здійснюватися в різні способи (зокрема у вигляді пам'ятки, на офіційному веб-сайті тощо).

Також власниками магазинів, ресторанів, торговельних центрів має бути забезпечено механізм розгляду запитів про доступ до персональних даних та іншої довідкової інформації.

⁸ Стаття 8 Закону України «Про захист персональних даних».

Що передбачає право на доступ до своїх персональних даних?

Людина має право на доступ до своїх персональних даних, зокрема знати процедури їх обробки.⁹ Такий запит можна зробити усно або письмово¹⁰ та безоплатно отримати відповідь¹¹.

Разом із тим важливо зазначити, що на практиці процедура забезпечення доступу до персональних даних має певні ризики, бо володільці інформації, отримавши такий запит, повинні бути впевнені в тому, що звернувся належний запитувач, а не стороння особа. Це означає, що володільці даних, щоб забезпечити належний захист інформації, можуть встановлювати свої процедури ідентифікації запитувача (наприклад, через відповідні коди доступу, просити надати дані особисто тощо).

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ІНФОРМАЦІЇ ЩОДО ОБРОБКИ ЙОГО ПЕРСОНАЛЬНИХ ДАНИХ

Найменування та адреса володільця персональних даних
Від кого (ПІБ особи запитувача) або законного представника
Реквізити документа, що посвідчує фізичну особу, яка подає запит¹²

ЗАПИТ
на отримання інформації щодо обробки персональних даних

Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені таку інформацію, що стосується обробки моїх персональних даних:

- відомості про володільця даних (найменування та місцезнаходження);
- підтвердження факту обробки моїх персональних даних, а також мету та законні підстави такої обробки;
- способи обробки моїх персональних даних, що застосовуються;
- відомості про осіб, які мають доступ до моїх персональних даних, зокрема тих, кому їх може бути передано;
- перелік оброблюваних персональних даних;
- терміни зберігання та процедури видалення моїх даних.

Дата, підпис

⁹ Стаття 8 Закону України «Про захист персональних даних».

¹⁰ Стаття 16 Закону України «Про захист персональних даних».

¹¹ Стаття 19 Закону України «Про захист персональних даних».

¹² Стаття 16 Закону України «Про захист персональних даних».

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ДОСТУПУ ДО ВІДЕОЗАПИСІВ, ЩО МІСТЯТЬ ЙОГО ПЕРСОНАЛЬНІ ДАНІ

<p style="text-align: center;"><u>Найменування та адреса володільця персональних даних</u> <u>Від кого (ПІБ особи запитувача) або законного представника</u> <u>Реквізити документа, що посвідчує фізичну особу, яка подає запит</u>¹³</p> <p style="text-align: center;">ЗАПИТ на отримання доступу до відеозаписів, що містять персональні дані</p> <p>Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені відеозаписи, що містять мої персональні дані в період _____.</p> <p><u>Дата, підпис</u></p>
--

Чи можна оприлюднювати записи з відеореєстраторів у мережі Інтернет?

Ураховуючи, що в зону відеоспостереження потрапляє багато людей, необхідно дотримуватися їхнього права на приватність. Це можна зробити за умови повної анонімізації, за винятком випадків, коли така інформація є предметом суспільного інтересу¹⁴.

Право на приватність не є абсолютним, проте будь-яке обмеження має бути аргументовано поєднанням таких умов:

- втручання у приватне життя здійснюється згідно із законом;
- втручання 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.

Що робити, якщо права порушені?

Звернутися безпосередньо до адміністрації (керівництва) магазину, ресторану (або іншого закладу) з вимогою про усунення порушення, пов'язаного із забезпеченням захисту персональних даних. Це краще зробити письмово, поштовим відправленням, щоб полігшити процедуру доведення факту звернення. Також можна оскаржити дії чи бездіяльність володільців даних до Уповноваженого або суду¹⁵.

¹³ Стаття 16 Закону України «Про захист персональних даних».

¹⁴ Відповідно до статті 29 Закону України «Про доступ до публічної інформації» предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

¹⁵ Стаття 22 Закону України «Про захист персональних даних».

Наприклад, якщо особа подала запит щодо даних про себе й отримала відмову, то обов'язок доведення в суді законності такої відмови покладається на володільця персональних даних, до якого подано запит¹⁶.

Чим передбачена відповідальність власника закладу за порушення вимог щодо захисту персональних даних?

Відповідальність передбачена:

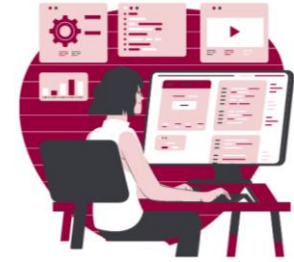
1. Кодексом України про адміністративні правопорушення (стаття 188-39 «Порушення законодавства у сфері захисту персональних даних»).
2. Кримінальним кодексом України (статті 182 «Порушення недоторканності приватного життя» та 359 «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»).

Відповідальність залежить від складу правопорушення.

¹⁶ Стаття 18 Закону України «Про захист персональних даних».

II. ВІДЕОСПОСТЕРЕЖЕННЯ В РАМКАХ ТРУДОВИХ ВІДНОСИН

Питання про встановлення відеоспостереження на робочому місці є дуже актуальним, оскільки багато роботодавців встановлюють системи для контролю. Встановлення відеокамер в офісах (інших приміщеннях та по периметру) може мати різні цілі: *збереження майна, безпека працівників та осіб, що перебувають у приміщенні, контроль доступу до документів тощо.*



В українському законодавстві недостатньо врегульовані процедури встановлення камер у рамках трудових відносин, зокрема широко дискутуються питання щодо балансу між приватністю людини й інтересами роботодавців стосовно контролю робочого процесу. Але у кожному разі необхідно враховувати право людини на приватність.



Чи можна встановлювати приховану камеру в офісі?

За загальним правилом — ні, можна здійснювати тільки відкриту відеозйомку. Тобто працівник має знати про відеокамери, а також бути повідомленим про такі умови праці¹⁷. Повідомлення має передбачати щонайменше:

- ✓ мету відеоспостереження;
- ✓ правову підставу відеоспостереження;
- ✓ параметри відеоспостереження: кількість, розташування та функціональні можливості відеокамер (наприклад, чи записується звук);
- ✓ час моніторингу;
- ✓ права суб'єктів персональних даних;
- ✓ порядок обробки та як захищена інформація;
- ✓ умови доступу до даних;
- ✓ термін зберігання та знищення даних.

Разом із тим роботодавці під час встановлення систем повинні враховувати принцип пропорційності, тобто попередньо оцінити в кожному окремому випадку, чи є інші доступні способи досягнення мети, окрім застосування відеоспостереження. Наприклад, наприкінці 2019 року Велика палата Європейського суду з прав людини (далі – ЄСПЛ) висловила позицію в рамках розгляду справи «Лопес Рібальда та інші проти Іспанії», яка стосувалася прихованого відеоспостереження за працівниками мережі супермаркетів, що призвело до звільнення тих із них, які викрадають речі.

Великою палатою ЄСПЛ зазначено, що заявники працювали в частині приміщення, яка є відкритою і, враховуючи, що спостереження було обмеженим у часі, а також, що лише окремі суб'єкти мали доступ до перегляду відеозаписів, ступінь втручання у право

¹⁷ Стаття 29 Кодексу законів про працю.

заявників на приватне життя не набув високого рівня. Також Велика палата звернула увагу, що відеозаписи були використані виключно для виявлення винних у недостахах осіб, і не було інших доступних заходів, за допомогою яких роботодавець міг би досягти мети, що полягала, зокрема, у захисті власності.

З огляду на це було констатовано відсутність порушення права на повагу до приватного і сімейного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод.

Велика палата ЄСПЛ визначила **критерії**, які повинні застосовуватися роботодавцями під час прийняття рішення про встановлення камер відеоспостереження на робочому місці, з урахуванням специфіки трудових відносин та розвитку нових технологій:



- **Чи повідомлений працівник про можливість встановлення роботодавцем відеоспостереження та про безпосередню реалізацію таких заходів?** На практиці працівники можуть бути повідомлені у різні способи залежно від конкретних обставин. Проте, за загальним правилом, працівник має бути повідомлений до початку запровадження відповідного моніторингу. Крім того, повідомлення має містити чітку інформацію щодо виду здійснюваного моніторингу.
- **В якому обсязі роботодавцем здійснюватиметься відеоспостереження та які межі втручання у приватне життя працівника?** Тобто, чи може працівник розумно розраховувати на приватність у зоні (приміщенні), яка підлягає відеоспостереженню, у комплексі із будь-якими обмеженнями у часі та просторі і кількістю осіб, що мають доступ до результатів моніторингу.
- **Чи навів роботодавець законні підстави для здійснення відеоспостереження, та чи повідомив про чіткі межі втручання?** Чим більше втручання передбачається, тим вагомішими мають бути підстави для його обґрунтування.
- **Чи можна було б запровадити систему контролю, яка передбачала б менше втручання?** Роботодавець має проводити попередню оцінку щодо того, чи можна досягти визначеної мети шляхом меншого втручання у приватне життя працівника.
- **Якими є наслідки відеоспостереження для конкретного працівника?** Роботодавець має враховувати, яким чином він використовує далі результати моніторингу та чи дозволили отримані результати роботодавцеві досягти мети, для якої були запроваджені ті чи інші заходи.
- **Чи забезпечено працівника відповідними гарантіями, коли заходи з моніторингу, встановлені роботодавцем, передбачають втручання у приватне життя?** Такі гарантії можуть, з-поміж іншого, включати надання роботодавцем інформації зацікавленим працівникам щодо факту запровадження відеоспостереження та меж втручання, повідомлення роботодавцем незалежного наглядового органу про встановлення такого заходу або забезпечення працівників можливістю подати заперечення або скаргу.

Відповідно до статті 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» практика ЄСПЛ є джерелом права в Україні. Це означає, що викладені критерії мають також враховуватися українськими роботодавцями з метою встановлення балансу між правом роботодавця на захист своєї власності та правом працівника на повагу до приватного життя.

Чи має роботодавець отримувати згоду від працівників на проведення зйомки?

Згода як підстава для обробки даних повинна бути вільною та добровільною. Тобто людині має бути гарантовано вибір та враховуватись її бажання: чи хоче вона, щоб за нею здійснювався відеоконтроль, чи — ні.

Роботодавцям некоректно отримувати згоду від працівників на проведення зйомки, бо це суперечитиме закону. У більшості випадків встановлення відеокамер аргументується роботодавцями — як умова праці та необхідність захисту своїх законних інтересів. Разом із тим варто пам'ятати, що така обробка даних буде законною лише тоді, коли встановлення відеокамер є обґрунтованим. Тобто особи, що приймають рішення про відеоспостереження, повинні оцінити, чи можна досягти визначених цілей іншими засобами. А також проаналізувати потенційний негативний вплив таких заходів на права і свободи людини. Якщо баланс інтересів не співмірний, роботодавцям варто шукати інші способи досягнення своїх цілей щодо відеоспостереження.



Як документально має бути закріплений такий вид контролю?

Роботодавець має щонайменше:

- провести оцінку законних інтересів та скласти про це відповідний документ, в якому: 1) описано законні цілі, яких буде досягнуто шляхом встановлення відеоспостереження, 2) обґрунтовано необхідність здійснення відеоспостереження та чому цілей неможливо досягти іншими засобами, що менше впливають на приватність, 3) зазначено заходи, спрямовані на забезпечення балансу прав працівників та роботодавця;
- внести пункт про відеоспостереження в Правила внутрішнього трудового розпорядку;
- скласти відповідний документ (яким може бути, зокрема «Політика приватності»), де буде роз'яснено порядок здійснення відеоспостереження, зокрема план розташування камер, їхні технічні особливості та додаткові функції, часові межі здійснення відеоспостереження тощо;
- зафіксувати факт ознайомлення співробітників з відповідними документами;
- видати наказ із зазначенням осіб, відповідальних за обробку даних, та осіб, що мають доступ до записів;
- забезпечити систематичне навчання відповідальних осіб для забезпечення належного рівня кваліфікації.

Де заборонено встановлювати відеокамери?

Заборонено встановлювати камери в туалетних кімнатах, душових, роздягальнях для персоналу та інших місцях, де людина може розраховувати на приватність. Також не варто ставити камери в приміщенні, де працює одна людина, оскільки це може розцінюватися як навмисний збір інформації про конкретну особу та мати на неї психологічний вплив. Звичайно, можуть бути обґрунтовані виключення, наприклад, коли йдеться про касу банку або пункт обміну валют, де такі заходи як відеоспостереження, виправдані не лише в інтересах роботодавців, а й з метою захисту працівників.



Які у вас є права щодо здійснення відеоспостереження?

Передусім ви маєте право¹⁸:

- знати назву (найменування) та місцезнаходження суб'єкта, що здійснює відеоспостереження;
- знати про законні підстави та джерела збирання даних (зокрема, розташування камер);
- знати про місцезнаходження своїх персональних даних (де знаходяться відеозаписи) та мету їх обробки;
- знати про умови надання доступу до своїх даних, зокрема інформацію про третіх осіб, яким вони передаються;
- отримувати не пізніше як за 30 календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, або обробляються ваші персональні дані, а також отримувати зміст таких персональних даних;
- пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням;
- право на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- знати механізм автоматизованої обробки персональних даних та мати захист від автоматизованого рішення, яке має для нього правові наслідки;
- отримувати інформацію про умови безпеки та обробки даних;
- отримувати інформацію про свої права та процедуру оскарження у разі їх порушення;
- отримувати контактну інформацію особи, визначеної роботодавцем відповідальною у даній сфері, для звернення з додатковими питаннями;
- звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або суду.

¹⁸ Стаття 8 Закону України «Про захист персональних даних».

Інформування про відеоспостереження може здійснюватися різними способами (зокрема, у вигляді пам'ятки, на офіційному веб-сайті тощо).

Що передбачає право на доступ до своїх даних?

Людина має право на доступ до своїх персональних даних, зокрема знати процедури їх обробки¹⁹. Такий запит можна зробити усно або письмово²⁰ та безоплатно отримати відповідь²¹.

Разом із тим важливо зазначити, що на практиці процедура забезпечення доступу до даних має певні ризики, бо володільці інформації, отримавши такий запит, повинні бути впевненими у тому, що звернувся належний запитувач, а не стороння особа. Це означає, що володільці даних, щоб забезпечити належний захист інформації, можуть встановлювати свої процедури ідентифікації запитувача (наприклад, через відповідні коди доступу, просити надати дані особисто тощо).

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ІНФОРМАЦІЇ ЩОДО ОБРОБКИ ЙОГО ПЕРСОНАЛЬНИХ ДАНИХ

Найменування та адреса володільця персональних даних
Від кого (ПІБ особи запитувача) або законного представника
Реквізити документа, що посвідчує фізичну особу, яка подає запит²²

ЗАПИТ
на отримання інформації щодо обробки персональних даних

Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені таку інформацію, що стосується обробки моїх персональних даних:

- відомості про володільця даних (найменування та місцезнаходження);
- підтвердження факту обробки моїх персональних даних, а також мету та законні підстави такої обробки;
- способи обробки моїх персональних даних, що застосовуються;
- відомості про осіб, які мають доступ до моїх персональних даних, зокрема тих, кому їх може бути передано;
- перелік оброблюваних персональних даних;
- терміни зберігання та процедури видалення моїх даних.

дата, підпис

¹⁹ Стаття 8 Закону України «Про захист персональних даних».

²⁰ Стаття 16 Закону України «Про захист персональних даних».

²¹ Стаття 19 Закону України «Про захист персональних даних».

²² Стаття 16 Закону України «Про захист персональних даних».

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ДОСТУПУ ДО ВІДЕОЗАПИСІВ, ЩО МІСТЯТЬ ЙОГО ПЕРСОНАЛЬНІ ДАНІ

<p style="text-align: center;"><u>Найменування та адреса володільця персональних даних</u> <u>Від кого (ПІБ особи запитувача) або законного представника</u> <u>Реквізити документа, що посвідчує фізичну особу, яка подає запит</u>²³</p> <p style="text-align: center;">ЗАПИТ на отримання доступу до відеозаписів, що містять персональні дані</p> <p>Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені відеозаписи, що містять мої персональні дані в період _____.</p> <p><u>Дата, підпис</u></p>
--

Що робити, якщо права порушені?

Звернутися безпосередньо до керівництва (роботодавця) з вимогою усунути порушення, пов'язані з забезпеченням права на захист персональних даних. Оскаржити дії чи бездіяльність роботодавця у цій сфері до Уповноваженого або суду²⁴.

Чим передбачена відповідальність роботодавця у разі порушення вимог щодо захисту персональних даних?

Відповідальність передбачена:

1. Кодексом України про адміністративні правопорушення (стаття 188-39 «Порушення законодавства у сфері захисту персональних даних»).
2. Кримінальним кодексом України (статті 182 «Порушення недоторканності приватного життя» та 359 «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»).

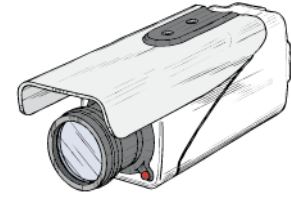
Разом із тим залежно від складу правопорушення може передбачатися відповідальність у рамках трудового законодавства. Зокрема, якщо людина не була належно поінформована про умови праці, де передбачалося постійне відеоспостереження.

²³ Стаття 16 Закону України «Про захист персональних даних».

²⁴ Стаття 22 Закону України «Про захист персональних даних».

III. ВІДЕОСПОСТЕРЕЖЕННЯ В БАГАТОПОВЕРХОВИХ БУДИНКАХ ТА НА ТЕРИТОРІЇ ЖИТЛОВИХ КОМПЛЕКСІВ

На сьогодні встановлення систем відеоспостереження в під'їздах багатоповерхових будинків та на території житлових комплексів стало необхідним атрибутом безпеки. Мешканці з власної ініціативи встановлюють камери, щоб контролювати внутрішні приміщення будинків і території загального користування.



Як правило, рішення про встановлення відеокамер приймаються спільно шляхом голосування співвласниками квартир на загальних зборах. Також є випадки, коли системи відеоспостереження території житлового комплексу є частиною плану забудовника. Проте незалежно від ініціатора жителі та відвідувачі будинків та житлових комплексів повинні мати змогу отримати інформацію про розташування камер, їх функціональні можливості, хто є володільцем таких технологій та щодо обсягу інформації, що збирається за їх допомогою, порядок обробки та доступу до даних.

Чи можна встановлювати камеру відеоспостереження в під'їзді?

Встановлювати камеру над власними дверима не заборонено. Необхідно погоджувати цей захід тоді, коли відеоспостереження охоплює сусідні вхідні двері або спільний сходовий майданчик.

З огляду на судову практику²⁵ встановлення камер спостереження без дозволу сусідів може бути оскаржено як порушення права людини на повагу до приватного та сімейного життя. Суд може прийняти рішення та зобов'язати особу, що встановила відеокамеру, демонтувати пристрій.

Під'їзд є місцем загального користування²⁶ та фактично прирівнюється до громадського місця, тому тут працюють ті самі правила, що діють у магазинах й торговельних центрах. Тому зйомка не може бути прихованою, люди повинні знати про встановлені камери.

Відеоспостереження, як і будь-які інші технічні засоби, повинні використовуватися залежно від мети: особисті/побутові потреби або професійні/комерційні потреби. Це означає, якщо цілі різняться від побутових, необхідно забезпечити вимоги законодавства у сфері захисту персональних даних.

Чи потрібен дозвіл на встановлення камери?

У разі якщо камери встановлюються на першому поверсі холу або на вході в під'їзд потрібно отримати дозвіл на встановлення від мешканців будинку (під'їзду). Це можна

²⁵ <https://www.uacourt.openregister.info/tsyvilni-spravy-z-01-01-2019-40297/spravy-pozovnogo-provadhennya-40298/spravy-u-sporakh-pro-zakhyst-nemaynovykh-prav-fizychnykh-osib-z-nykh-40364/pro-zakhyst-chesti-gidnosti-ta-dilovoyi-reputatsiyi-z-nykh-40365?document=91863727>

²⁶ Стаття 15 Закону України «Про об'єднання співвласників багатоквартирних будинків».

зробити шляхом проведення загальних зборів, на яких має бути прийнято рішення не тільки про закупівлю камер, а й порядок їх встановлення, розташування та обробки інформації, що буде збиратися за їх допомогою.

Зокрема, визначається відповідальна особа за захист персональних даних та виконання законодавства у даній сфері. Також потрібно розробити документ, що встановлює порядок обробки інформації (Політику приватності), та ознайомити з ним усіх мешканців, які проживають у цьому під'їзді й потенційно можуть перебувати у зоні спостереження.

Що має містити такий документ (Політика приватності)?

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.

Інформування про відеоспостереження може здійснюватися у різні способи (наприклад, у вигляді пам'ятки, таблички або на офіційному веб-сайті). Також має бути забезпечений механізм розгляду запитів про доступ до персональних даних та іншої довідкової інформації.

Які права мають жителі та відвідувачі будинку/житлового комплексу?

Передусім мають право²⁷:



- знати назву (найменування) та місцезнаходження суб'єкта, що здійснює відеоспостереження;
- знати про законні підстави та джерела збирання даних (зокрема розташування камер);
- знати про місцезнаходження своїх персональних даних (де знаходяться відеозаписи) та мету їх обробки;
- знати про умови надання доступу до своїх даних, зокрема інформацію про третіх осіб, яким вони передаються;
- отримувати не пізніше як за 30 календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються персональні дані, а також отримувати зміст таких персональних даних;
- пред'являти вмотивовану вимогу із запереченням проти обробки своїх персональних даних;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням;
- право на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- знати механізм автоматизованої обробки персональних даних та мати захист від автоматизованого рішення, яке має для нього правові наслідки;
- отримувати інформацію про умови безпеки та обробки даних;
- отримувати інформацію про свої права та процедуру оскарження у разі їх порушення;
- отримувати контактну інформацію, до кого можна звернутися з додатковими питаннями у даній сфері;
- звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або суду.

²⁷ Стаття 8 Закону України «Про захист персональних даних».

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ІНФОРМАЦІЇ ЩОДО ОБРОБКИ ЙОГО ПЕРСОНАЛЬНИХ ДАНИХ

Найменування та адреса володільця персональних даних
Від кого (ПІБ особи запитувача) або законного представника
Реквізити документа, що посвідчує фізичну особу, яка подає запит²⁸

ЗАПИТ

на отримання інформації щодо обробки персональних даних

Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені таку інформацію, що стосується обробки моїх персональних даних:

- відомості про володільця даних (найменування та місцезнаходження);
- підтвердження факту обробки моїх персональних даних, а також мету та законні підстави такої обробки;
- способи обробки моїх персональних даних, що застосовуються;
- відомості про осіб, які мають доступ до моїх персональних даних, зокрема тих, кому їх може бути передано;
- перелік оброблюваних персональних даних;
- терміни зберігання та процедури видалення моїх даних;

Дата, підпис

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ДОСТУПУ ДО ВІДЕОЗАПИСІВ, ЩО МІСТЯТЬ ЙОГО ПЕРСОНАЛЬНІ ДАНІ:

Найменування та адреса володільця персональних даних
Від кого (ПІБ особи запитувача) або законного представника
Реквізити документа, що посвідчує фізичну особу, яка подає запит²⁹

ЗАПИТ

на отримання доступу до відеозаписів, що містять персональні дані

Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені відеозаписи, що містять мої персональні дані в період _____.

Дата, підпис

²⁸ Стаття 16 Закону України «Про захист персональних даних».

²⁹ Стаття 16 Закону України «Про захист персональних даних».

Чи є правомірним встановлення відеокамер на території приватного будинку?

Люди мають право запроваджувати різні заходи безпеки своєї приватної власності, зокрема встановлювати системи відеоспостереження. Не застосовуються положення Закону України «Про захист персональних даних», якщо така обробка здійснюється фізичною особою виключно для особистих чи побутових потреб³⁰.

Проте, якщо зона відеоспостереження охоплює територію сусіднього приватного будинку й така зйомка ведеться без дозволу, в такому разі це може вважатися порушенням права на приватне та сімейне життя іншої людини.

Якщо камера охоплює територію загального користування (наприклад дорогу), тобто громадські місця, необхідно встановити попереджувальний знак, що ведеться відеоспостереження.

Що робити, якщо права порушені?

1. Звернутися з вимогою усунути порушення, пов'язані з забезпеченням прав на захист персональних даних, до ОСББ або особи, яка за спільним рішенням співвласників будинку визначена відповідальною за використання системи та обробки даних, отриманих за її допомогою (у разі якщо створено ОСББ).
2. Звернутися до керуючої компанії, яка розміщувала системи відеоспостереження та забезпечує приватну охорону житлового комплексу.
3. Оскаржити дії чи бездіяльність володільців даних до Уповноваженого або суду³¹.

³⁰ Стаття 25 Закону України «Про захист персональних даних».

³¹ Стаття 22 Закону України «Про захист персональних даних».

IV. КАМЕРИ ВІДЕОФІКСАЦІЇ НА ДОРОГАХ ТА В ГРОМАДСЬКОМУ ТРАНСПОРТІ



Масштаби дорожньо-транспортного травматизму в Україні є катастрофічними. Основна причина — перевищення дозволеної швидкості руху транспортного засобу. У 2020 році на українських дорогах запрацювала система фіксації в автоматичному режимі адміністративних правопорушень у сфері безпеки дорожнього руху.

Система фіксує порушення Правил дорожнього руху за допомогою стаціонарних технічних засобів. Технічні вимоги до системи затверджує Міністерство внутрішніх справ (далі — МВС України). Впровадження приладів контролю на автомобільних дорогах загального користування державного значення покладено на власників таких доріг, а на автомобільних дорогах загального користування місцевого значення, вулицях і дорогах у містах та інших населених пунктах — на органи місцевого самоврядування.

Інформування учасників дорожнього руху про фіксацію (фото- або відеозапис) адміністративних порушень здійснюється на визначених місцях через встановлення відповідних дорожніх знаків, а також шляхом розміщення відомостей на офіційних веб-сайтах МВС та Національної поліції України³².

Місця встановлення приладів контролю погоджуються з уповноваженим органом Національної поліції України, а саме — Департаментом патрульної поліції. Користувачами системи є:

- **реєстратор** — посадова особа уповноваженого підрозділу Національної поліції України, яка здійснює обробку інформаційних файлів, інформаційну взаємодію з іншими органами державної влади, а також виносить, змінює, скасовує постанови про накладення адміністративного стягнення;
- **адміністратор** — посадова особа уповноваженого підрозділу МВС України, яка забезпечує супроводження програмного забезпечення, збереження та захист даних системи, відповідає за її належне функціонування, надання доступу до системи та обмін даними з іншими інформаційними системами та реєстрами.

Після фіксації події Системою інформація надходить до центру обробки даних Департаменту патрульної поліції та розглядається уповноваженим поліцейським, з урахуванням відомостей, отриманих з відповідних баз даних (реєстрів), необхідних для винесення постанови про накладення адміністративного стягнення. Володільцем баз даних, якими користується Національна поліція України, є — МВС України. Також поліція використовує бази даних Міністерства юстиції України, Державної прикордонної служби України та інших³³.

³² Постанова Кабінету Міністрів України «Про функціонування системи фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі». <https://zakon.rada.gov.ua/laws/show/833-2017-п#Text>

³³ Наприклад, Єдиний державний реєстр транспортних засобів, Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань.

Поліція має безпосередній оперативний доступ до інформаційних ресурсів органів державної влади за умови обов'язкового дотримання Закону України «Про захист персональних даних»³⁴.

Проблема полягає в тому, що згідно з законодавством та відповідно до Конституції України притягнення до відповідальності людини має індивідуальний характер, а також діє презумпція невинуватості. Це означає, що саме на державний орган покладається обов'язок доведення, хто керував автотранспортним засобом під час вчинення правопорушення. Оскільки часто складно ідентифікувати особу, яка була за кермом, є випадки, коли люди отримують помилкові повідомлення про штраф. Використання особистої інформації фізичної особи має здійснюватися тільки законно та для конкретних цілей. Зокрема, людина має право на захист від надання відомостей, що є недостовірними чи ганьблять її честь, гідність та ділову репутацію. Це означає, що особа, отримавши недостовірну інформацію, має право звернутися до адресата з проханням щодо її виправлення або уточнення, а також на захист від автоматизованого рішення, яке має для неї правові наслідки³⁵.

Чи збирають персональні дані за допомогою відеокamer на дорогах?

За допомогою відеозапису можна прямо або опосередковано ідентифікувати фізичну особу — її риси обличчя, параметри тіла тощо. Наприклад, якщо людину, яка перебуває в автомобілі, можна конкретно впізнати, тоді це вважатиметься прямою ідентифікацією; якщо через державний номерний знак автомобіля — непрямою ідентифікацією (опосередкованою).

Також за допомогою системи відеоспостереження можна дізнатися марку автомобіля, періоди пересування, маршрути в місті тощо, що сукупно може надати широкий спектр приватної інформації про людину та її приватне життя.

Чи правомірно встановлюють відеокamери у громадському транспорті?

Наразі поширеною є практика облаштування системами відеоспостереження громадський транспорт. Також бортові камери ще встановлюють у поїздах та приміських електричках. Як правило, це здійснюють різні суб'єкти, наприклад, органи місцевого самоврядування та «Укрзалізниця». Заходи відеоспостереження обґрунтовуються необхідністю посилення безпеки пасажирів і водіїв.

Станом на сьогодні існують проблеми правового регулювання щодо встановлення систем відеоспостереження з боку місцевої влади, оскільки у профільному Законі України «Про місцеве самоврядування в Україні» відсутні прямі повноваження щодо встановлення технологій стеження за населенням. Разом із тим, ураховуючи реформу децентралізації, жителі громад часто самі стають ініціаторами впровадження відеоспостереження для підтримки суспільної безпеки. Про це свідчить зміст локальних програм, які приймають більшість місцевих рад. Щодо громадського транспорту, то муніципалітети (інші суб'єкти) доволі часто обґрунтовують встановлення бортових відеокamer необхідністю захисту законних інтересів щодо забезпечення правопорядку та збереження власності громади.

³⁴ Стаття 27 Закону України «Про Національну поліцію».

³⁵ Стаття 8 Закону України «Про захист персональних даних».

Як і в будь-якому громадському місці, тут працюють ті самі правила щодо відкритості ведення зйомки. Тобто має бути розміщено на видному місці напис про те, що «ведеться відеоспостереження». Враховуючи, що камери у громадському транспорті встановлюють різні суб'єкти, то відповідно й володільці даних також будуть різні. Все залежить від того, де та ким встановлено камеру.

Хто несе відповідальність за порядок обробки та захисту даних?

Як зазначено раніше, відеоспостереження на дорогах або громадському транспорті встановлюють багато суб'єктів, які можуть мати різні законні підстави, цілі та повноваження. Це означає, що сфера відповідальності залежатиме від того, ким встановлено камеру.

Уповноваженим офіційно було надано рекомендації для усіх суб'єктів, що встановлюють відеокамери, у яких, з-поміж іншого, було рекомендовано забезпечити можливість ідентифікувати, кому належать встановлені відеокамери та яка мета відеоспостереження. Це означає, що поряд із інформацією про факт здійснення відеоспостереження відповідне повідомлення має містити інформацію про власника камери та мету.



УВАГА!
Здійснюється відеоспостереження для підтримання порядку!

Контакти відповідальної особи: Для більш детальної інформації:
00-000-000



Чи можна публікувати запис із камер відеоспостереження в мережі Інтернет?

Поширена практика, коли записи з фіксацією дорожньо-транспортних пригод публікуються у мережі Інтернет для поширення новин. На запис потрапляють постраждалі особи або інші люди, які випадково там опинилися. З позиції законодавства про захист персональних даних — це може вважатися порушенням права людини на приватність.

У результаті дорожньо-транспортної пригоди особа може зазнати фізичних або емоційних страждань, тому публікація її зображення на широкий загал може завдати їй ще більшої шкоди. Поширення персональних даних без згоди людини можливе лише для захисту її життєво-важливих інтересів або з метою оперативно-розшукової діяльності (фото порушника, який втік із місця події).

Наприклад, терміново потрібно ідентифікувати особу, щоб знайти її близьких або надати медичну допомогу, або інцидент становить суспільний інтерес.

Разом із тим це не означає, що публікувати новину не потрібно. Це варто робити за умови повної анонімізації, крім винятків, коли така інформація не може бути конфіденційною відповідно до закону. Кожна людина має право на повагу до власного приватного життя, тому в кожному випадку необхідно забезпечити дотримання балансу між суспільним інтересом та правом на приватність.

Які права мають учасники дорожнього руху щодо захисту своїх персональних даних у зв'язку зі здійсненням відеоспостереження?



Передусім³⁶:

- знати назву (найменування) та місцезнаходження суб'єкта, що здійснює відеоспостереження;
- знати про законні підстави та джерела збирання даних (зокрема, місця розташування камер);
- знати про місцезнаходження своїх персональних даних (де знаходяться відеозаписи) та мету їх обробки;
- знати про умови надання доступу до своїх даних, зокрема інформацію про третіх осіб, яким вони передаються;
- отримувати не пізніше як за 30 календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються персональні дані, а також отримувати зміст таких персональних даних;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням;
- право на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- знати механізм автоматизованої обробки персональних даних та мати захист від автоматизованого рішення, яке має для нього правові наслідки;
- отримувати інформацію про умови безпеки та обробки даних;
- отримувати інформацію про свої права та процедуру оскарження у разі їх порушення;
- отримувати контактну інформацію, до кого можна звернутися з додатковими питаннями у даній сфері;
- звертатися зі скаргами на обробку своїх персональних даних до Уповноваженого або суду.

Інформування про відеоспостереження може здійснюватися у різні способи (*наприклад, у вигляді таблички, на офіційному веб-сайті тощо*). З адресами камер фото-відеофіксації можна ознайомитися на сайті Міністерства внутрішніх справ України. Також володільці мають забезпечити відповідний механізм розгляду запитів про доступ до персональних даних та іншої довідкової інформації.

³⁶ Стаття 8 Закону України «Про захист персональних даних».

Що передбачає право на доступ до персональних даних?

У статті 8 Закону України «Про захист персональних даних» зазначено, що суб'єкт персональних даних має право на доступ до своїх даних, зокрема процедури їх обробки. Особи можуть зробити такий запит як усно, так і письмово³⁷. Доступ особи до персональних даних здійснюється безоплатно³⁸.

Разом із тим зазначимо, що на практиці процедура забезпечення доступу до персональних даних має певні ризики, бо володільці інформації, отримавши такий запит, повинні бути впевнені в тому, що звернувся належний запитувач, а не стороння особа. Це означає, що володільці даних, щоб забезпечити належних захист інформації, можуть встановлювати свої процедури ідентифікації запитувача (наприклад, через відповідні коди доступу, просити надати дані особисто тощо).

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ІНФОРМАЦІЇ ЩОДО ОБРОБКИ ЙОГО ПЕРСОНАЛЬНИХ ДАНИХ

<p><u>Найменування та адреса володільця персональних даних</u> <u>Від кого (ПІБ особи запитувача) або законного представника</u> <u>Реквізити документа, що посвідчує фізичну особу, яка подає запит</u>³⁹</p> <p>ЗАПИТ на отримання інформації щодо обробки персональних даних</p> <p>Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені таку інформацію, що стосується обробки моїх персональних даних:</p> <ul style="list-style-type: none"> ● відомості про володільця даних (найменування та місцезнаходження); ● підтвердження факту обробки моїх персональних даних, а також мету та законні підстави такої обробки; ● способи обробки моїх персональних даних, що застосовуються; ● відомості про осіб, які мають доступ до моїх персональних даних, зокрема тих, кому їх може бути передано; ● перелік оброблюваних персональних даних; ● терміни зберігання та процедури видалення моїх даних. <p><u>Дата, підпис</u></p>
--

³⁷ Стаття 16 Закону України «Про захист персональних даних».

³⁸ Стаття 19 Закону України «Про захист персональних даних».

³⁹ Стаття 16 Закону України «Про захист персональних даних».

ФОРМА ЗАПИТУ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ НА ОТРИМАННЯ ДОСТУПУ ДО ВІДЕОЗАПИСІВ, ЩО МІСТЯТЬ ЙОГО ПЕРСОНАЛЬНІ ДАНІ

<p style="text-align: center;"><u>Найменування та адреса володільця персональних даних</u> <u>Від кого (ПІБ особи запитувача) або законного представника</u> <u>Реквізити документа, що посвідчує фізичну особу, яка подає запит</u>⁴⁰</p> <p style="text-align: center;">ЗАПИТ на отримання доступу до відеозаписів, що містять персональні дані</p> <p>Відповідно до статей 8, 16, 19 Закону України «Про захист персональних даних» з метою _____ прошу надати мені відеозаписи, що містять мої персональні дані в період _____.</p> <p><u>Дата, підпис</u></p>
--

Такі запити має бути задоволено, крім випадків, коли обмеження у наданні такої інформації прямо передбачено законом.

Коли ви можете бути не повідомлені про дії з вашими персональними даними?

Повідомлення не здійснюється у разі:

1. Передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом.
2. Виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом.
3. Здійснення обробки даних з історичною, статистичною чи науковою метою.

Що робити, якщо права порушені?

Звернутися з вимогою усунути порушення, пов'язані з забезпеченням прав на захист персональних даних, можна безпосередньо до установи, яка встановила системи відеоспостереження та здійснює обробку даних. Також можна оскаржити дії чи бездіяльність такої установи до Уповноваженого або суду⁴¹.

⁴⁰ Стаття 16 Закону України «Про захист персональних даних».

⁴¹ Стаття 22 Закону України «Про захист персональних даних».