Європейська рада із захисту даних

Настанови

Настанови 3/2019 щодо обробки персональних даних за допомогою відеопристроїв

Версія 2.0

Прийнято 29 січня 2020 року

Прийнято

Історія версій

Версія 2.1	26 лютого 2020 року	Виправлення суттєвих помилок
Версія 2.0	29 січня 2020 року	Прийняття Настанов після публічних консультацій
Версія 1.0	10 липня 2019 року	Прийняття Настанов для публічних консультацій

Прийнято

Зміст

Прийнято

Прийнято

Цей переклад не є офіційним перекладом Європейської ради із захисту даних. Переклад здійснено за фінансової підтримки GIZ у рамках Регіонального проєкту «Реформа державного управління в країнах Східного партнерства III» та тісній співпраці з Офісом Уповноваженого Верховної Ради України з прав людини та Європейською радою із захисту даних. Правильність перекладу підтверджено Офісом Уповноваженого Верховної Ради України з прав людини

ЄВРОПЕЙСЬКА РАДА ІЗ ЗАХИСТУ ДАНИХ

Беручи до уваги статтю 70(1)(e) Регламенту Європейського Парламенту та Ради 2016/679/ЄС від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (далі — «GDPR»).

Беручи до уваги Угоду про ЄЕП, зокрема, Додаток XI та Протокол 37 до неї, зі змінами, внесеними Рішенням Спільного Комітету ЄЕП № 154/2018 від 6 липня 2018 року[1],

Беручи до уваги статтю 12 та статтю 22 його Регламенту,

ПРИЙНЯЛА ТАКІ НАСТАНОВИ

1 ВСТУП

1. Інтенсивне використання відеопристроїв впливає на поведінку громадян. Значне впровадження таких інструментів у багатьох сферах життя громадян створюватиме додатковий тиск на особу з метою запобігання виявленню того, що може бути сприйнято як відхилення. Де-факто, ці технології можуть обмежити можливості анонімного пересування та анонімного користування послугами й загалом обмежити можливість залишитися непоміченим. Наслідки для захисту даних є значними.

2. Хоча окремі особи можуть бути задоволені відеоспостереженням, встановленим, наприклад, з певною метою безпеки, необхідно вжити заходів для уникнення будь-якого зловживання для зовсім інших і неочікуваних для суб'єкта даних цілей (зокрема маркетингових цілей, моніторингу ефективності роботи працівників тощо). Крім того, зараз впроваджено багато інструментів для використання знятих зображень і перетворення традиційних камер на «розумні» камери. Обсяг даних, що генеруються відео, у поєднанні із цими інструментами та методами збільшує ризики вторинного використання (незалежно від того, чи пов'язане воно з початковою метою системи) або навіть ризики зловживань. Загальні принципи, викладені в GDPR (стаття 5), завжди слід ретельно враховувати при роботі з відеоспостереженням.

3. Системи відеоспостереження багато в чому змінюють спосіб взаємодії професіоналів з приватного та державного секторів у приватних або громадських місцях з метою посилення безпеки, отримання аналізу аудиторії, надання персоналізованої реклами тощо.

[1] Посилання на «держави-члени», що містяться в цьому висновку, слід розуміти як посилання на «держави-члени ЄЕП».

Прийнято

Відеоспостереження стало високоефективним завдяки зростаючому впровадженню інтелектуального відеоаналізу. Ці методи можуть бути більш інтрузивними (наприклад, складні біометричні технології) або менш інтрузивними (наприклад, прості алгоритми підрахунку). Залишатися анонімним і зберігати конфіденційність загалом стає дедалі складніше. Питання захисту даних, що виникають у кожній ситуації, можуть відрізнятися, так само як і правовий аналіз при використанні тієї чи іншої технології.

4. Окрім питань конфіденційності, існують також ризики, пов'язані з можливими збоями в роботі цих пристроїв та упередженнями, які вони можуть викликати. Дослідники повідомляють, що програмне забезпечення, яке використовується для ідентифікації, розпізнавання або аналізу обличчя, працює по-різному залежно від віку, статі та етнічної приналежності особи, яку воно ідентифікує. Алгоритми працюватимуть на основі різних демографічних даних, а отже, упередженість у розпізнаванні облич загрожує посиленням упереджень у суспільстві. Саме тому контролери даних повинні також забезпечити, щоб обробка біометричних даних, отриманих за допомогою відеоспостереження, підлягала регулярній оцінці на предмет її релевантності та достатності наданих гарантій.

5. Відеоспостереження не є необхідністю за замовчуванням, коли існують інші засоби для досягнення основної мети. В іншому випадку ми ризикуємо змінити культурні норми, що призведе до прийняття відсутності приватного життя як загального принципу.

6. Ці настанови мають на меті надати рекомендації щодо застосування GDPR у зв'язку з обробкою персональних даних за допомогою відеопристроїв. Наведені приклади не є вичерпними, загальні міркування можуть бути застосовані до всіх потенційних сфер використання.

Прийнято

2 СФЕРА ЗАСТОСУВАННЯ[2]

2.1 Персональні дані

7. Систематичне автоматизоване спостереження певного простору за допомогою оптичних або аудіовізуальних засобів, здебільшого з метою захисту власності або захисту життя та здоров'я людей, стало важливим явищем сьогодення. Ця діяльність полягає у зборі та збереженні візуальної або аудіовізуальної інформації про всіх осіб, які входять у простір, що контролюється, і можуть бути ідентифіковані на основі їхньої зовнішності або інших окремих ознак. На основі цих даних можна встановити цих осіб. Це також уможливлює подальшу обробку персональних даних про присутність і поведінку осіб у даному просторі. Потенційний ризик неправомірного використання цих даних зростає зі збільшенням розміру контрольованого простору, а також кількості осіб, які його відвідують. Цей факт відображений у Загальному регламенті про захист даних у статті 35(3)(c), яка вимагає оцінки впливу на захист даних у разі систематичного та широкомасштабного моніторингу зони, що знаходиться у відкритому доступі, а також у статті 37(1)(b), яка вимагає від операторів призначити відповідального за захист даних, якщо операція з обробки за своїм характером передбачає регулярний і систематичний моніторинг суб'єктів даних.

8. Однак Регламент не застосовується до обробки даних, які не пов'язані з особою, наприклад, якщо фізична особа не може бути ідентифікована, прямо чи опосередковано.

> Приклад: GDPR не застосовується до фейкових камер (тобто будь-якої камери, яка не функціонує як камера і, відповідно, не обробляє жодних персональних даних). *Однак у деяких державах-членах на них може поширюватися інше законодавство.*
>
> Приклад: Записи з великої висоти підпадають під сферу дії GDPR лише в тому випадку, якщо за певних обставин оброблені дані можуть бути пов'язані з конкретною особою.
>
> Приклад: Відеокамера встановлена в автомобіль для надання допомоги при паркуванні. Якщо камера сконструйована або налаштована таким чином, що вона не збирає жодної інформації, пов'язаної з фізичною особою (наприклад, номерні знаки або інформацію, яка може ідентифікувати перехожих), GDPR не застосовується.

9.

[2] Європейська рада із захисту даних («EDPB») зазначає, що там, де це дозволяє GDPR, можуть застосовуватися конкретні вимоги національного законодавства.

Прийнято

2.2 Застосування Директиви ЄС про правоохоронні органи (2016/680)

10. Зокрема, обробка персональних даних компетентними органами з метою попередження, розслідування, виявлення або переслідування кримінальних правопорушень чи виконання кримінальних покарань, включаючи захист та запобігання загрозам громадській безпеці, підпадає під дію Директиви ЄС № 2016/680.

2.3 Винятки для домогосподарств

11. Відповідно до статті 2(2)(c) обробка персональних даних фізичною особою під час суто особистої або домашньої діяльності, яка також може включати діяльність в Інтернеті, не підпадає під сферу дії GDPR.[3]

12. Це положення — так званий виняток для домогосподарств — у контексті відеоспостереження повинно тлумачитися обмежено. Таким чином, як вважає Суд ЄС, так званий «виняток для домогосподарств» повинен *«тлумачитися як такий, що стосується лише діяльності, яка здійснюється під час приватного або сімейного життя фізичних осіб, що явно не стосується обробки персональних даних, яка полягає в публікації в Інтернеті у спосіб, коли ці дані стають доступними невизначеному колу осіб»*. [4] Крім того, якщо система відеоспостереження передбачає постійний запис і зберігання персональних даних та охоплює, *«навіть частково, громадський простір, тобто спрямована назовні з приміщення приватної особи, яка здійснює обробку даних, вона не може вважатися суто «приватною або сімейною» діяльністю для цілей другого абзацу статті 3(2) Директиви 95/46»*[5].

13. Що стосується відеопристроїв, які використовуються в приміщенні приватної особи, то вони можуть підпадати під виняток для домогосподарств. Це буде залежати від декількох факторів, які необхідно враховувати для того, щоб дійти висновку. Окрім вищезазначених елементів, визначених у рішеннях Суду ЄС, користувачеві відеоспостереження в домашніх умовах необхідно звернути увагу на те, чи має він особисті стосунки із суб'єктом даних, чи вказує масштаб або частота спостереження на певну професійну діяльність з його боку, а також на потенційний негативний вплив спостереження на суб'єктів даних. Наявність будь-якого одного з вищезазначених елементів не обов'язково свідчить про те, що обробка не підпадає під дію винятку для домогосподарств, для такого визначення необхідна загальна оцінка.

---

[3] Див. також преамбулу 18.

[4] Суд ЄС, рішення у справі C-101/01, *справа Боділа Ліндквіста*, 6 листопада 2003 року, п. 47.

[5] Суд ЄС, рішення у справі C-212/13, *«Франтішек Ринеш проти Управління з питань захисту персональних даних»*, 11 грудня 2014 року, п. 33.

Прийнято

Приклад: Турист записує відео на мобільний телефон і відеокамеру, щоб задокументувати свою відпустку. Він показує відзнятий матеріал друзям і родині, але не робить його доступним для невизначеного кола осіб. Це підпадає під виняток для домогосподарств.

Приклад: Гірська велосипедистка, яка спускається з гори, хоче записати свій спуск на екшн-камеру. Вона катається у віддаленій місцевості та планує використовувати записи лише для особистої розваги вдома. Це підпадає під виняток для домогосподарств, навіть якщо певною мірою здійснюється обробка персональних даних.

Приклад: Хтось спостерігає та записує свій власний сад. Територія огороджена, і лише сам контролер і його сім'я регулярно відвідують сад. Це підпадає під виняток для домогосподарств за умови, що відеоспостереження не поширюється навіть частково на громадський простір або сусідню власність.

14.

3 ЗАКОННІСТЬ ОБРОБКИ

15. Перед використанням необхідно детально визначити цілі обробки (стаття 5(1)(b)). Відеоспостереження може слугувати багатьом цілям, наприклад, підтримці захисту майна та інших активів, підтримці захисту життя та фізичної недоторканності осіб, збору доказів для цивільних позовів. [6] Ці цілі моніторингу мають бути задокументовані в письмовій формі (стаття 5(2)) і визначені для кожної камери спостереження, що використовується. Камери, які використовуються з тією ж метою одним контролером, можуть бути задокументовані разом. Крім того, суб'єкти даних повинні бути поінформовані про цілі обробки відповідно до статті 13 (*див. розділ 7 «Зобов'язання щодо прозорості інформації»*). Відеоспостереження, засноване лише на цілі «безпеки» або «для вашої безпеки», не є достатньо конкретним (стаття 5(1)(b)). Крім того, це суперечить принципу, що персональні дані повинні оброблятися у законний, правомірний і прозорий спосіб щодо суб'єкта даних (див. статтю 5(1)(a)).

16. У цілому кожна правова підстава, передбачена статтею 6(1), може забезпечити законну підставу для обробки даних відеоспостереження. Наприклад, стаття 6(1)(c) застосовується, якщо національне законодавство передбачає обов'язок здійснювати відеоспостереження.[7] Однак на практиці найчастіше застосовуються такі положення:

    - стаття 6(1)(f) (законні інтереси),

[6] Правила збору доказів для цивільних позовів у державах-членах ЄС можуть відрізнятися.

[7] Ці настанови не аналізують і не заглиблюються в деталі національного законодавства, яке може відрізнятися в різних державах-членах ЄС.

Прийнято

- стаття 6(1)(e) (необхідність виконання завдання в суспільних інтересах або для здійснення офіційних повноважень).

У досить виняткових випадках стаття 6(1)(a) (надання згоди) може бути використана контролером як законна підстава.

3.1 Законні інтереси, стаття 6(1)(f)

17. Правова оцінка статті 6(1)(f) повинна ґрунтуватися на наступних критеріях відповідно до преамбули 47.

3.1.1 Наявність законних інтересів

18. Відеоспостереження є законним, якщо воно необхідне для досягнення цілей законних інтересів, переслідуваних контролером або третьою стороною, якщо тільки такі інтереси не переважають інтереси суб'єкта даних або основоположні права й свободи (стаття 6(1)(f)). Законні інтереси, які переслідує контролер або третя сторона, можуть бути правовими [8], економічними або нематеріальними.[9] Однак контролер повинен враховувати, що якщо суб'єкт даних заперечує проти спостереження відповідно до статті 21, контролер може продовжувати відеоспостереження за цим суб'єктом даних, лише якщо це є *вагомим* законним інтересом, який переважає інтереси, права й свободи суб'єкта даних або для встановлення, здійснення або захисту правових претензій.

19. Враховуючи реальну та небезпечну ситуацію, мета захисту майна від злому, крадіжки або вандалізму може становити законний інтерес для відеоспостереження.

20. Законний інтерес повинен існувати реально та бути актуальною проблемою (тобто він не повинен бути вигаданим або спекулятивним) [10]. Перед початком спостереження має бути реальна ситуація, що викликає занепокоєння, наприклад, збитки або серйозні інциденти в минулому. У світлі принципу підзвітності контролерам рекомендується задокументувати відповідні інциденти (дата, спосіб, фінансові втрати) та пов'язані з ними кримінальні звинувачення. Ці задокументовані інциденти можуть бути вагомим доказом існування законного інтересу. Існування законного інтересу, а також необхідність моніторингу слід переоцінювати через певні проміжки часу (наприклад, раз на рік, залежно від обставин).

---

[8] Суд ЄС, рішення у справі C-13/16, *справа Rīgas satiksme*, 4 травня 2017 року

[9] див. РД 217, Робоча група за статтею 29.

[10] див. РД 217, Робоча група за статтею 29, с. 24 і далі див. також справу Суду ЄС C-708/18, с. 44

Прийнято

Приклад: Власник магазину хоче відкрити новий магазин і встановити систему відеоспостереження для запобігання вандалізму. Він може показати, представивши статистичні дані, що в найближчому районі існує високий ризик вандалізму. Також корисним є досвід сусідніх магазинів. Необов'язково, щоб відповідний контролер даних зазнав шкоди. Достатньо, щоб пошкодження по сусідству свідчили про небезпеку або щось подібне, а отже, могли бути ознакою законного інтересу. Однак недостатньо представити національну або загальну статистику злочинності без аналізу району, про який ідеться, або небезпеки для цього конкретного магазину.

21.

22. Ситуації безпосередньої небезпеки можуть становити законний інтерес, зокрема банки або магазини, що продають дорогоцінні товари (наприклад, ювелірні), або райони, які, як відомо, є типовими місцями скоєння злочинів проти власності (наприклад, автозаправні станції).

23. GDPR також чітко визначає, що органи державної влади не можуть покладатися на обробку даних на підставі законного інтересу, якщо вони виконують свої завдання, стаття 6(1), речення 2.

3.1.2 Необхідність обробки

24. Персональні дані повинні бути достатніми та відповідними й обмежуватися лише їхньою мірою необхідності з огляду на цілі обробки («мінімізація даних»), див. статтю 5(1)(c). Перед встановленням системи відеоспостереження контролер завжди повинен критично оцінити, чи є цей захід, по-перше, придатним для досягнення бажаної мети, а по-друге, належним і необхідним для її цілей. Заходи відеоспостереження слід обирати лише тоді, коли мета обробки не може бути обґрунтовано досягнута іншими засобами, які є менш інтрузивними для основоположних прав та свобод суб'єкта даних.

25. Враховуючи ситуацію, коли контролер хоче запобігти майновим злочинам, замість встановлення системи відеоспостереження, він може також вжити альтернативних заходів безпеки, як-от огородження території, регулярне патрулювання персоналом служби безпеки, використання сторожа, забезпечення кращого освітлення, встановлення захисних замків, захищених від злому вікон і дверей або нанесення на стіни покриття чи плівки проти графіті. Ці заходи можуть бути настільки ж ефективними, як і системи відеоспостереження для захисту від злому, крадіжок і вандалізму. У кожному конкретному випадку контролер повинен оцінити, чи є такі заходи обґрунтованим рішенням.

26. Перед початком експлуатації системи відеоспостереження контролер повинен оцінити, чи заходи відеоспостереження є вкрай необхідними. Зазвичай система відеоспостереження, що працює в нічний час, а також у неробочий час, відповідає потребам контролера, щоб запобігти будь-якій небезпеці для його майна.

Прийнято

27. Загалом, необхідність використання відеоспостереження для захисту приміщень контролерів закінчується за межами їхньої власності.[11] Однак існують випадки, коли для ефективного захисту майна недостатньо лише відеоспостереження за його межами. У деяких окремих випадках може виникнути потреба у розширенні відеоспостереження до безпосереднього оточення приміщення. У цьому контексті контролер повинен розглянути фізичні й технічні засоби, як-от блокування або пікселювання несуттєвих ділянок.

> Приклад: Книгарня хоче захистити своє приміщення від вандалізму. Загалом, камери повинні знімати лише саме приміщення, оскільки для цього немає потреби спостерігати за сусідніми приміщеннями або громадськими місцями навколо приміщення книгарні.

28.

29. Питання щодо необхідності обробки також виникають стосовно способу збереження доказів. У деяких випадках може виникнути необхідність у використанні «чорних скриньок», коли відзнятий матеріал автоматично видаляється після певного терміну зберігання і доступ до нього надається лише у випадку інциденту. В інших ситуаціях, можливо, взагалі не потрібно записувати відеоматеріал, а доцільніше використовувати моніторинг у режимі реального часу. Обрання між рішеннями «чорних скриньок» і моніторингом у режимі реального часу також має ґрунтуватися на меті, яку ви переслідуєте. Якщо, наприклад, метою відеоспостереження є збереження доказів, методи моніторингу в режимі реального часу зазвичай не підходять. Іноді моніторинг у режимі реального часу може бути більш інтрузивним, ніж зберігання та автоматичне видалення матеріалів через обмежений проміжок часу (наприклад, якщо хтось постійно дивиться на монітор, це може бути більш інтрузивним, ніж якби монітор взагалі був відсутній, а матеріали зберігалися б безпосередньо в «чорній скриньці»). У цьому контексті слід розглядати принцип мінімізації даних (стаття 5(1)(c)). Слід також мати на увазі, що контролер може використовувати персонал служби безпеки замість відеоспостереження, який здатний негайно відреагувати й втрутитися в ситуацію.

3.1.3 Баланс інтересів

30. Припускаючи, що відеоспостереження необхідне для захисту законних інтересів контролера, система відеоспостереження може бути введена в експлуатацію лише в тому випадку, якщо законні інтереси контролера або третіх осіб (наприклад, захист власності або фізичної недоторканності) не переважають над інтересами або основоположними правами й свободами суб'єкта даних. Контролер повинен враховувати: 1) якою мірою моніторинг зачіпає інтереси, основоположні права та свободи фізичних осіб, та 2) чи не спричиняє це порушення або негативні

[11] У деяких державах-членах це також може регулюватися національним законодавством.

наслідки щодо прав суб'єкта даних. Фактично, дотримання балансу інтересів є обов'язковим. Основоположні права та свободи, з одного боку, та законні інтереси контролера, з іншого боку, повинні бути ретельно оцінені та збалансовані.

Приклад: Приватна паркувальна компанія задокументувала періодичні проблеми з крадіжками припаркованих автомобілів. Місце для паркування є відкритим простором і може бути легко доступним для будь-кого, але воно чітко позначене знаками та дорожніми блокіраторами, що оточують простір. Паркувальна компанія має законний інтерес (запобігання крадіжкам автомобілів клієнтів) контролювати територію в той час доби, коли виникають проблеми з крадіжками. За суб'єктами даних ведеться спостереження в обмежений проміжок часу, вони перебувають на території не з метою відпочинку, і в їхніх власних інтересах також є запобігання крадіжкам. Інтереси суб'єктів даних, які не підлягають моніторингу, в цьому випадку переважають над законним інтересом контролера.

Приклад: Ресторан вирішує встановити відеокамери в туалетах, щоб контролювати чистоту санітарних приміщень. У цьому випадку права суб'єктів даних явно переважають над інтересом контролера, тому камери не можуть бути встановлені в цих місцях.

31.

3.1.3.1 Прийняття рішень у кожному конкретному випадку

32. Оскільки баланс інтересів є обов'язковим відповідно до регламенту, рішення має прийматися в кожному конкретному випадку (див. статтю 6(1)(f)). Недостатньо посилатися на абстрактні ситуації або порівнювати подібні випадки між собою. Контролер повинен оцінити ризики порушення прав суб'єкта даних; тут вирішальним критерієм є інтенсивність втручання в права та свободи особи.

33. Інтенсивність може, серед іншого, визначатися типом інформації, яка збирається (зміст інформації), обсягом (щільність інформації, просторовий та географічний масштаб), кількістю суб'єктів даних, яких це стосується, як конкретної кількості, так і частки відповідного населення, ситуацією, про яку йдеться, реальними інтересами групи суб'єктів даних, альтернативними засобами, а також характером та обсягом оцінки даних.

34. Важливими факторами балансу можуть бути розмір території, яка перебуває під спостереженням, та кількість суб'єктів даних, які перебувають під спостереженням. Використання відеоспостереження у віддаленій місцевості (наприклад, для спостереження за дикою природою або для захисту критичної інфраструктури, як-от приватної радіоантени) має оцінюватися інакше, ніж відеоспостереження в пішохідній зоні або торговому центрі.

Прийнято

Приклад: Якщо встановлюється відеореєстратор (наприклад, з метою збору доказів у разі ДТП), важливо переконатися, що ця камера не записує постійно рух транспорту, а також осіб, які перебувають поблизу дороги. Інакше інтерес до відеозаписів як доказів у більш теоретичному випадку ДТП не може виправдати таке серйозне втручання у права суб'єктів даних.[11]

35.

3.1.3.2 Обґрунтовані очікування суб'єктів даних

36. Відповідно до преамбули 47, існування законного інтересу потребуватиме ретельного оцінювання. При цьому необхідно враховувати обґрунтовані очікування суб'єкта даних на момент і в контексті обробки його персональних даних. Що стосується систематичного моніторингу, то відносини між суб'єктом даних та контролером можуть суттєво відрізнятися та впливати на те, які обґрунтовані очікування може мати суб'єкт даних. Інтерпретація поняття «обґрунтовані очікування» повинна ґрунтуватися не лише на суб'єктивних очікуваннях, про які йдеться. Скоріше, вирішальним критерієм має бути те, чи могла б об'єктивна третя сторона обґрунтовано очікувати та зробити висновок про те, що вона підлягає моніторингу в цій конкретній ситуації.

37. Наприклад, працівник на своєму робочому місці в більшості випадків не очікує, що його роботодавець буде здійснювати моніторинг.[12] Крім того, не варто очікувати моніторингу у власному саду, в житлових приміщеннях або в кабінетах для обстеження та лікування. Так само не варто очікувати моніторингу в санітарно-гігієнічних приміщеннях або саунах: моніторинг таких зон є суттєвим втручанням у права суб'єкта даних. Обґрунтовані очікування суб'єктів даних полягають у тому, що відеоспостереження в цих місцях не буде здійснюватися. З іншого боку, клієнт банку може очікувати, що за ним стежитимуть у приміщенні банку або біля банкомата.

38. Суб'єкти даних також можуть розраховувати на відсутність моніторингу в загальнодоступних місцях, особливо якщо ці місця зазвичай використовуються для відпочинку, релаксації та проведення дозвілля, а також у місцях, де люди перебувають та/або спілкуються, таких як зони відпочинку, столики в ресторанах, парках, кінотеатрах та фітнес-центрах. Тут інтереси або права та свободи суб'єкта даних часто переважають над законними інтересами контролера.

Приклад: У туалетах суб'єкти даних очікують, що за ними не стежитимуть. Відеоспостереження, наприклад, для запобігання нещасним випадкам, не є пропорційним.

39.

[12] Див. також Робоча група за статтею 29, Висновок 2/2017 щодо обробки даних на робочому місці, РД 249, прийнятий 8 червня 2017 року.

Прийнято

40. Знаки, що інформують суб'єкта даних про відеоспостереження, не мають значення при визначенні того, чого об'єктивно може очікувати суб'єкт даних. Це означає, що, наприклад, власник магазину не може покладатися на те, що покупці *об'єктивно* мають обґрунтовані очікування щодо спостереження лише тому, що табличка на вході інформує особу про відеоспостереження.

3.2 Необхідність виконання завдання в суспільних інтересах або для здійснення офіційних повноважень, покладених на контролера, стаття 6(1)(e)

41. Персональні дані можуть оброблятися за допомогою відеоспостереження відповідно до статті 6(1)(e), якщо це необхідно для виконання завдання в суспільних інтересах або для здійснення офіційних повноважень.[13] Може статися так, що здійснення офіційних повноважень не дозволяє таку обробку, але інші законодавчі підстави, такі як «охорона здоров'я та безпека» для захисту відвідувачів та працівників, можуть забезпечити обмежений обсяг обробки, але з урахуванням зобов'язань за GDPR та прав суб'єктів даних.

42. Держави-члени можуть підтримувати або запроваджувати окреме національне законодавство щодо відеоспостереження для адаптації застосування правил GDPR шляхом більш точного визначення конкретних вимог до обробки, якщо це відповідає принципам, викладеним у GDPR (наприклад, обмеження зберігання, пропорційність).

3.3 Надання згоди, стаття 6(1)(a)

43. Згода має надаватися вільно, бути конкретною, інформованою та недвозначною, як описано в настановах щодо надання згоди.[14]

44. Що стосується систематичного моніторингу, то згода суб'єкта даних може слугувати законною підставою відповідно до статті 7 (див. преамбулу 43) лише у виняткових випадках. За своєю природою ця технологія спостереження є спостереженням за невідомою кількістю людей одночасно. Контролер навряд чи зможе довести, що суб'єкт даних надав згоду на обробку своїх персональних даних (стаття 7(1)). Якщо припустити, що суб'єкт даних відкликає свою згоду, контролеру буде важко довести, що персональні дані більше не обробляються (стаття 7(3)).

---

[13] «Підстави для такої обробки встановлюються законодавством Союзу або законодавством держави-члена» та «є необхідними для виконання завдання в суспільних інтересах або для здійснення офіційних повноважень, покладених на контролера» (стаття 6(3)).

[14] «Настанови щодо надання згоди відповідно до Регламенту 2016/679» Робочої групи за статтею 29 (РД 259, версія 01). – схвалені EDPB
Прийнято

Приклад: Спортсмени можуть вимагати моніторингу під час виконання окремих вправ, щоб проаналізувати свою техніку та результати. З іншого боку, якщо спортивний клуб виступає з ініціативою моніторингу всієї команди з тією ж метою, згода часто не буде дійсною, оскільки окремі спортсмени можуть відчувати тиск, щоб їхня відмова від згоди не вплинула негативно на товаришів по команді.

45.

46. Якщо контролер хоче покладатися на згоду, він зобов'язаний переконатися, що кожен суб'єкт даних, який входить у зону, що перебуває під відеоспостереженням, надав свою згоду. Ця згода повинна відповідати умовам статті 7. Вхід у позначену зону спостереження (наприклад, людей запрошують пройти через певний коридор або ворота, щоб увійти в зону спостереження) не є заявою або чіткою позитивною дією, необхідною для отримання згоди, якщо вона не відповідає критеріям статей 4 і 7, як це описано в настановах щодо надання згоди.[15]

47. Враховуючи дисбаланс влади між роботодавцями та працівниками, у більшості випадків роботодавці не повинні покладатися на згоду при обробці персональних даних, оскільки вона навряд чи буде надана добровільно. У цьому контексті слід враховувати настанови щодо надання згоди.

48. Законодавство держав-членів або колективні договори, в тому числі «трудові угоди», можуть передбачати конкретні правила обробки персональних даних працівників у контексті трудових відносин (див. статтю 88).

4 РОЗКРИТТЯ ВІДЕОМАТЕРІАЛІВ ТРЕТІМ ОСОБАМ

49. У цілому загальні положення GDPR застосовуються до розкриття відеозаписів третім особам.

4.1 Розкриття відеозаписів третім особам у цілому

50. Розкриття визначається в статті 4(2) як передача (наприклад, індивідуальне повідомлення), розповсюдження (наприклад, публікація в Інтернеті) або надання доступу в інший спосіб. Треті сторони визначені у статті 4(10). Якщо розкриття інформації здійснюється третім країнам або міжнародним організаціям, застосовуються також окремі положення статті 44 і далі.

51. Будь-яке розкриття персональних даних є окремим видом обробки персональних даних, для якої контролер повинен мати законну підставу, передбачену статтею 6.

[15] «Настанови щодо надання згоди відповідно до Регламенту 2016/679» Робочої групи за статтею 29 (РД 259) – схвалені EDPB – необхідно взяти до уваги.
Прийнято

Приклад: Контролер, який бажає завантажити запис в Інтернет, повинен покладатися на законну підставу для такої обробки, наприклад, отримати згоду суб'єкта даних відповідно до статті 6(1)(a).

52.

53. Передача відеозаписів третім особам з іншою метою, ніж та, для якої були зібрані дані, можлива відповідно до правил статті 6(4).

Приклад: Відеоспостереження за шлагбаумом (на автостоянці) встановлено з метою врегулювання збитків. Виникає пошкодження, і запис передається адвокату для ведення справи. У цьому випадку мета запису така ж, як і мета передачі.

Приклад: Відеоспостереження за шлагбаумом (на автостоянці) встановлено з метою врегулювання збитків. Запис публікується в Інтернеті з метою розваги. У цьому випадку мета змінилася і є несумісною з початковою метою. Крім того, було б проблематично визначити законну підставу для такої обробки (публікації).

54.

55. Третій стороні-одержувачу доведеться провести власний правовий аналіз, зокрема, визначити законну підставу за статтею 6 для своєї обробки (наприклад, отримання матеріалу).

4.2 Передача відеоматеріалів правоохоронним органам

56. Передача відеозаписів правоохоронним органам також є самостійним процесом, який вимагає окремого обґрунтування для контролера.

57. Згідно зі статтею 6(1)(c), обробка є законною, якщо вона необхідна для виконання юридичного зобов'язання, яке має контролер. Хоча застосовне законодавство у сфері правоохоронної діяльності знаходиться під виключним контролем держав-членів, імовірно, існують загальні правила, які регулюють передачу доказів правоохоронним органам у кожній державі-члені. Обробка даних, що передаються контролером, регулюється GDPR. Якщо національне законодавство вимагає від контролера співпрацювати з правоохоронними органами (наприклад, під час розслідування), законною підставою для передачі даних є юридичне зобов'язання згідно зі статтею 6(1)(c).

58. Обмеження щодо мети, передбачене статтею 6(4), часто не викликає проблем, оскільки розкриття інформації чітко відсилає нас до законодавства держави-члена. Тому немає потреби розглядати окремі вимоги щодо зміни мети в сенсі пунктів «a»–«e».

Прийнято

Приклад: Власник магазину записує відео на вході до нього. На відеозаписі видно, як людина краде гаманець іншої людини. Поліція просить контролера передати матеріал, щоб допомогти в розслідуванні. У цьому випадку власник магазину використовує законну підставу, передбачену статтею 6(1)(c) (юридичне зобов'язання), у поєднанні з відповідним національним законодавством для обробки передачі.

59.

Приклад: У магазині встановлюють камеру з міркувань безпеки. Власник магазину вважає, що він зафіксував щось підозріле на відеозаписі, і вирішує надіслати матеріал до поліції (без жодних ознак того, що ведеться якесь розслідування). У цьому випадку власник магазину повинен оцінити, чи дотримані умови, передбачені в більшості випадків статтею 6(1)(f). Зазвичай це відбувається, якщо власник магазину має обґрунтовану підозру, що було скоєно злочин.

60.

61. Обробка персональних даних самими правоохоронними органами не підпадає під дію GDPR (див. статтю 2(2)(d)), а натомість підпадає під дію Директиви ЄС про правоохоронні органи (2016/680).

5 ОБРОБКА СПЕЦІАЛЬНИХ КАТЕГОРІЙ ДАНИХ

62. Системи відеоспостереження зазвичай збирають величезні обсяги персональних даних, які можуть містити дані дуже особистого характеру й навіть спеціальні категорії даних. Таким чином, на перший погляд, незначні дані, зібрані за допомогою відео, можуть бути використані для отримання іншої інформації для досягнення іншої мети (наприклад, для складання карти звичок людини). Однак відеоспостереження не завжди вважається обробкою особливих категорій персональних даних.

Приклад: Відеоматеріали, на яких суб'єкт даних носить окуляри або користується інвалідним візком, самі по собі не вважаються особливими категоріями персональних даних.

63.

64. Однак, якщо обробка відеоматеріалів здійснюється для виведення особливих категорій даних, застосовується стаття 9.

Приклад: Політичні погляди можна, наприклад, вивести із зображень, на яких суб'єкти даних, яких можна ідентифікувати, беруть участь у заході, страйку тощо. Це підпадає під дію статті 9.

Приклад: Встановлення лікарнею відеокамери для спостереження за станом здоров'я пацієнта буде розглядатися як обробка особливих категорій персональних даних (стаття 9).

65.

Прийнято

66. Загалом, як правило, при встановленні системи відеоспостереження слід ретельно враховувати принцип мінімізації даних. Таким чином, навіть у випадках, коли стаття 9(1) не застосовується, контролер даних завжди повинен намагатися мінімізувати ризик того, що відеозапис розкриє інші конфіденційні дані (що виходять за рамки статті 9), незалежно від мети.

> Приклад: Відеоспостереження за церквою саме по собі не підпадає під дію статті 9. Однак контролер повинен провести особливо ретельну оцінку відповідно до статті 6(1)(f), беручи до уваги характер даних, а також ризик захоплення інших конфіденційних даних (за межами статті 9) при оцінці інтересів суб'єкта даних.

67.

68. Якщо система відеоспостереження використовується для обробки спеціальних категорій даних, контролер даних повинен визначити як виняток для обробки спеціальних категорій даних відповідно до статті 9 (тобто виняток із загального правила, що не можна здійснювати обробку спеціальних категорій даних), так і законну підставу відповідно до статті 6.

69. Наприклад, стаття 9(2)(c) («[...] *обробка необхідна для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи* [...]») може — теоретично та у виняткових випадках — використовуватися, але контролер даних повинен буде обґрунтувати це як абсолютну необхідність для захисту життєво важливих інтересів особи та довести, що цей «[...] суб'єкт даних *фізично або юридично не здатний надати свою згоду*». Крім того, контролеру даних не буде дозволено використовувати систему з будь-якої іншої причини.

70. Тут важливо зазначити, що кожен виняток, перерахований у статті 9, навряд чи може бути використаний для виправдання обробки спеціальних категорій даних за допомогою відеоспостереження. Зокрема, контролери даних, які здійснюють обробку цих даних у контексті відеоспостереження, не можуть посилатися на статтю 9(2)(e), яка дозволяє обробку персональних даних, що явно оприлюднені суб'єктом даних. Сам факт входження в зону дії камери не означає, що суб'єкт даних має намір оприлюднити особливі категорії даних, що його стосуються.

71. Крім того, обробка особливих категорій даних вимагає підвищеної та постійної пильності щодо дотримання певних зобов'язань; наприклад, високого рівня безпеки та оцінки впливу на захист даних, де це необхідно.

> Приклад: Роботодавець не повинен використовувати записи відеоспостереження, що показують демонстрацію, для ідентифікації учасників страйку.

72.

5.1 Загальні міркування при обробці біометричних даних

73. Використання біометричних даних і, зокрема, розпізнавання облич тягне за собою підвищені ризики для прав суб'єктів даних. Вкрай важливо, щоб використання таких технологій відбувалося з належним дотриманням принципів законності, необхідності, пропорційності та мінімізації Прийнято

даних, викладених у GDPR. Хоча використання цих технологій може сприйматися як особливо ефективне, контролери повинні насамперед оцінювати вплив на фундаментальні права й свободи та розглядати менш інтрузивні засоби для досягнення законної мети обробки даних.

74. Для того, щоб кваліфікуватися як біометричні дані згідно з визначенням GDPR, обробка необроблених даних, таких як фізичні, фізіологічні або поведінкові характеристики фізичної особи, має передбачати оцінювання цих характеристик. Оскільки біометричні дані є результатом таких оцінювань, у статті 4(14) GDPR зазначено, що вони «*[...] отримані в результаті спеціальної технічної обробки, яка стосується фізичних, фізіологічних чи поведінкових ознак фізичної особи, що дозволяють однозначно ідентифікувати або підтверджують однозначну ідентифікацію фізичної особи; [...]».* Однак відеозапис фізичної особи сам по собі не може вважатися біометричними даними відповідно до статті 9, якщо він не був спеціально технічно оброблений з метою сприяння ідентифікації фізичної особи. [16]

75. Для того, щоб це кваліфікувалося як обробка спеціальних категорій персональних даних (стаття 9), необхідно, щоб обробка біометричних даних здійснювалася «з метою однозначної ідентифікації фізичної особи».

76. Підсумовуючи, у світлі статей 4(14) та 9, необхідно враховувати три критерії:

- **Характер даних:** дані, що стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи;
- **Засоби та спосіб обробки**: дані, «отримані в результаті конкретної технічної обробки»;
- **Мета обробки:** дані повинні використовуватися з метою однозначної ідентифікації фізичної особи.

77. Використання систем відеоспостереження з функцією біометричного розпізнавання, встановлених приватними суб'єктами для власних цілей (наприклад, маркетингових, статистичних або навіть для забезпечення безпеки), у більшості випадків вимагатиме прямої згоди всіх суб'єктів даних (стаття 9(2)(a)), однак може застосовуватися й інший відповідний виняток у статті 9.

[16] Преамбула 51 GDPR підтримує цей аналіз, зазначаючи, що «*[...] Обробку фотографій не можна систематично вважати обробкою спеціальних категорій персональних даних, оскільки термін «біометричні дані» на них поширюється, лише якщо їх обробляють за допомогою спеціальних технічних засобів, що дозволяють однозначну ідентифікацію або автентифікацію фізичної особи. [...]*».
Прийнято

Приклад: Для покращення своїх послуг приватна компанія замінює пункти ідентифікації пасажирів в аеропорту (здача багажу, посадка) системами відеоспостереження, які використовують методи розпізнавання облич для перевірки особи пасажирів, які надали згоду на таку процедуру. Оскільки обробка підпадає під дію статті 9, пасажири, які заздалегідь надали свою явну та інформовану згоду, повинні будуть зареєструватися, наприклад, через автоматичний термінал, щоб створити та зберегти свій шаблон обличчя, пов'язаний із посадковим талоном та ідентифікаційними даними. Пункти контролю з розпізнаванням обличчя повинні бути чітко відокремлені. Наприклад, систему слід встановлювати всередині порталу, щоб унеможливити зняття біометричних шаблонів осіб, які не надали на це згоди. Тільки ті пасажири, які попередньо надали свою згоду та пройшли реєстрацію, зможуть користуватися турнікетом, обладнаним біометричною системою.

Приклад: Контролер керує доступом до своєї будівлі за допомогою методу розпізнавання облич. Люди можуть користуватися цим способом доступу, лише якщо вони заздалегідь надали свою явну та інформовану згоду (відповідно до статті 9(2)(a)). Однак для того, щоб гарантувати, що ніхто, хто раніше не надав своєї згоди, не буде охоплений, метод розпізнавання обличчя повинен запускатися самим суб'єктом даних, наприклад, шляхом натискання кнопки. Для забезпечення законності обробки контролер завжди повинен пропонувати альтернативний спосіб доступу до будівлі без обробки біометричних даних, наприклад, бейджі або ключі.

78.

79. У таких випадках, коли створюються біометричні шаблони, контролери повинні забезпечити, щоб після отримання результату збігу або відсутності збігу всі проміжні шаблони, створені «на льоту» (за явної та інформованої згоди суб'єкта даних) для порівняння з шаблонами, створеними суб'єктами даних під час реєстрації, були негайно та надійно видалені. Шаблони, створені для набору, повинні зберігатися лише для реалізації мети обробки й не повинні зберігатися або архівуватися.

80. Однак, якщо метою обробки є, зокрема, відрізнити одну категорію осіб від іншої, а не однозначно ідентифікувати будь-яку особу, обробка не підпадає під дію статті 9.

Приклад: Власник магазину хоче налаштувати свою рекламу на основі статевих і вікових характеристик покупців, зафіксованих системою відеоспостереження. Якщо ця система не генерує біометричні шаблони для однозначної ідентифікації особи, а лише виявляє ці фізичні характеристики з метою класифікації особи, то обробка не підпадає під дію статті 9 (за умови, що не здійснюється обробка інших видів спеціальних категорій даних).

81.

82. Однак стаття 9 застосовується, якщо контролер зберігає біометричні дані (найчастіше за допомогою шаблонів, які створюються шляхом вилучення ключових характеристик з необробленої форми біометричних даних (наприклад, виміри обличчя із зображення)) з метою однозначної ідентифікації особи. Якщо контролер бажає виявити суб'єкта даних, який

Прийнято

повертається на територію або в'їжджає в іншу територію (наприклад, для продовження показу персоналізованої реклами), метою буде унікальна ідентифікація фізичної особи, а це означає, що операція із самого початку підпадатиме під дію статті 9. Це може статися, якщо контролер зберігає згенеровані шаблони для подальшого розміщення персоналізованої реклами на кількох білбордах у різних місцях всередині магазину. Оскільки система використовує фізичні характеристики для виявлення конкретних осіб, які повертаються в зону дії камери (наприклад, відвідувачів торгового центру), і відстеження їх, це буде методом біометричної ідентифікації, оскільки він спрямований на розпізнавання за допомогою спеціальної технічної обробки.

Приклад: Власник магазину встановив систему розпізнавання облич у своєму магазині, щоб налаштувати рекламу для окремих осіб. Контролер даних повинен отримати чітку та інформовану згоду всіх суб'єктів даних, перш ніж використовувати цю біометричну систему та надавати персоналізовану рекламу. Система буде незаконною, якщо вона фіксуватиме відвідувачів або перехожих, які не давали згоди на створення їхнього біометричного шаблону, навіть якщо їхній шаблон буде видалено в найкоротший термін. Адже ці тимчасові шаблони є біометричними даними, які обробляються з метою однозначної ідентифікації особи, яка, можливо, не бажає отримувати таргетовану рекламу.

83.

84. EDPB зазначає, що деякі біометричні системи встановлюються в неконтрольованих середовищах[17], що означає, що система передбачає захоплення на льоту обличчя будь-якої особи, яка проходить в зоні дії камери, в тому числі осіб, які не дали згоди на використання біометричного пристрою, і, таким чином, створення біометричних шаблонів. Ці шаблони порівнюються з шаблонами, створеними суб'єктами даних, які надали попередню згоду під час реєстрації (тобто користувачами біометричних пристроїв), для того, щоб контролер даних міг розпізнати, чи є особа користувачем біометричного пристрою. У цьому випадку система часто розроблена таким чином, щоб відрізняти осіб, яких вона хоче розпізнати в базі даних, від тих, хто не зареєстрований. Оскільки метою є унікальна ідентифікація фізичних осіб, виняток згідно зі статтею 9(2) GDPR все одно застосовується для всіх осіб, яких знімають камери.

[17] Це означає, що біометричний пристрій знаходиться у відкритому для громадськості просторі та може спрацювати на будь-кого, хто проходить повз, на відміну від біометричних систем у контрольованому середовищі, які можуть бути використані лише за згодою особи, яка їх використовує.

Прийнято

Приклад: Готель використовує відеоспостереження для автоматичного сповіщення менеджера готелю про прибуття VIP-персони, коли розпізнається обличчя гостя. Ці VIP-персони заздалегідь надали свою явну згоду на використання розпізнавання обличчя перед тим, як їхні дані були занесені до бази даних, створеної для цієї мети. Такі системи обробки біометричних даних будуть незаконними, якщо всі інші гості, за якими ведеться спостереження (з метою ідентифікації VIP-персон), не дадуть згоди на обробку відповідно до статті 9(2)(a) GDPR.

Приклад: Контролер встановлює систему відеоспостереження з функцією розпізнавання облич на вході до концертного залу, яким він керує. Контролер повинен встановити чітко відокремлені входи: один з біометричною системою, а інший без неї (де ви, наприклад, скануєте квиток). Входи, обладнані біометричними пристроями, повинні бути встановлені та доступні таким чином, щоб система не могла зняти біометричні шаблони глядачів, які не дають на це згоди.

85.

86. Нарешті, коли згода вимагається статтею 9 GDPR, контролер даних не повинен обумовлювати доступ до своїх послуг згодою на обробку біометричних даних. Іншими словами, зокрема, коли обробка біометричних даних використовується з метою автентифікації, контролер даних повинен запропонувати альтернативне рішення, яке не передбачає обробку біометричних даних — без обмежень або додаткових витрат для суб'єкта даних. Таке альтернативне рішення також необхідне для осіб, які не відповідають обмеженням біометричного пристрою (неможливість реєстрації або зчитування біометричних даних, функціональні обмеження, що ускладнюють використання тощо), а також у випадку, коли біометричний пристрій недоступний (наприклад, несправність пристрою), має бути впроваджено «резервне рішення» для забезпечення безперервності пропонованої послуги, обмежене, однак, винятковим використанням. У виняткових випадках може виникнути ситуація, коли обробка біометричних даних є основною діяльністю послуги, що надається за договором, наприклад, у музеї, який організовує виставку для демонстрації використання пристрою розпізнавання облич, і в цьому випадку суб'єкт даних не зможе відмовитися від обробки біометричних даних, якщо він бажає взяти участь у виставці. У такому випадку згода, що вимагається статтею 9, залишається дійсною, якщо дотримані вимоги статті 7.

5.2 Запропоновані заходи для мінімізації ризиків при обробці біометричних даних

87. Відповідно до принципу мінімізації даних, контролери даних повинні гарантувати, що дані, витягнуті із цифрового зображення для побудови шаблону, не будуть надмірними та міститимуть лише інформацію, необхідну для зазначеної мети, таким чином уникаючи будь-якої можливої подальшої обробки. Необхідно вжити заходів, щоб гарантувати, що шаблони не можуть бути передані між біометричними системами.

Прийнято

88. Ідентифікація та автентифікація/верифікація, ймовірно, вимагатимуть зберігання шаблону для подальшого порівняння. Контролер даних повинен розглянути найбільш придатне місце для зберігання даних. У контрольованому середовищі (розмежовані коридори або контрольно-пропускні пункти) шаблони повинні зберігатися на індивідуальному пристрої, що перебуває у користувача та знаходиться під його виключним контролем (у смартфоні або ідентифікаційній картці), або, якщо це необхідно для конкретних цілей і за наявності об'єктивних потреб, зберігатися в централізованій базі даних у зашифрованому вигляді, доступ до якого можливий лише за допомогою криптографічного ключа/пароля, що знаходиться виключно в руках цієї особи, щоб запобігти несанкціонованому доступу до шаблону або місця зберігання. Якщо контролер даних не може уникнути доступу до шаблонів, він повинен вжити відповідних заходів для забезпечення безпеки даних, що зберігаються. Це може включати шифрування шаблону за допомогою криптографічного алгоритму.

89. У будь-якому випадку, контролер повинен вживати всіх необхідних запобіжних заходів для збереження доступності, цілісності та конфіденційності даних, що обробляються. З цією метою контролер повинен, зокрема, вжити таких заходів: розділяти дані під час передачі та зберігання, зберігати біометричні шаблони та необроблені дані або ідентифікаційні дані в окремих базах даних, шифрувати біометричні дані, зокрема біометричні шаблони, та визначити політику шифрування й управління ключами, впровадити організаційні й технічні заходи для виявлення шахрайства, пов'язати код цілісності з даними (наприклад, цифровий підпис або хеш-функція) та заборонити будь-який зовнішній доступ до біометричних даних. Такі заходи повинні вдосконалюватися з розвитком технологій.

90. Крім того, контролери даних повинні видалити необроблені дані (зображення обличчя, мовних сигналів, ходи тощо) та забезпечити ефективність цього видалення. Якщо більше немає законних підстав для обробки, необроблені дані мають бути видалені. Оскільки біометричні шаблони походять від таких даних, можна вважати, що створення баз даних може становити рівну, якщо не більшу загрозу (оскільки не завжди легко зчитати біометричний шаблон без знання того, як він був запрограмований, тоді як необроблені дані будуть будівельними блоками будь-якого шаблону). Якщо контролеру даних необхідно зберігати такі дані, необхідно вивчити методи з додаванням шуму (наприклад, водяні знаки), які зроблять створення шаблону неефективним. Контролер також повинен видаляти біометричні дані та шаблони в разі несанкціонованого доступу до термінала зчитування-порівняння або сервера зберігання даних, а також видаляти будь-які дані, які не є корисними для подальшої обробки в кінці терміну служби біометричного пристрою.

6 ПРАВА СУБ'ЄКТА ДАНИХ

91. У зв'язку з характером обробки даних при використанні відеоспостереження деякі права суб'єкта даних відповідно до GDPR потребують подальшого роз'яснення. Однак ця глава не є вичерпною,

всі права, передбачені GDPR, застосовуються до обробки персональних даних за допомогою відеоспостереження.

6.1 Право на доступ

92. Суб'єкт даних має право отримати від контролера підтвердження того, чи обробляються його персональні дані. У випадку відеоспостереження це означає, що якщо дані не зберігаються та не передаються жодним чином, то після завершення моніторингу в режимі реального часу контролер може лише надати інформацію про те, що персональні дані більше не обробляються (окрім загальних інформаційних зобов'язань відповідно до статті 13, див. *розділ 7 «Зобов'язання щодо прозорості інформації»).* Якщо, однак, дані все ще обробляються на момент запиту (тобто, якщо дані зберігаються або безперервно обробляються в будь-який інший спосіб), суб'єкт даних повинен отримати доступ та інформацію відповідно до статті 15.

93. Однак існує низка обмежень, які в деяких випадках можуть застосовуватися до права на доступ.

- Стаття 15(4) GDPR, це не повинно негативно впливати на права інших осіб

94. Враховуючи, що будь-яка кількість суб'єктів даних може бути записана в одній і тій же послідовності відеоспостереження, перегляд може призвести до додаткової обробки персональних даних інших суб'єктів даних. Якщо суб'єкт даних бажає отримати копію матеріалу (стаття 15(3)), це може негативно вплинути на права та свободи інших суб'єктів даних, що містяться в цьому матеріалі. Щоб запобігти цьому, контролер повинен враховувати, що через інтрузивний характер відеоматеріалів контролер не повинен у деяких випадках роздавати відеоматеріали, на яких можуть бути ідентифіковані інші суб'єкти даних. Однак захист прав третіх осіб не повинен використовуватися як виправдання для запобігання законним вимогам доступу з боку фізичних осіб, контролер повинен у таких випадках вжити технічних заходів для виконання запиту на доступ (наприклад, редагування зображення, як-от маскування або шифрування). Однак контролери не зобов'язані вживати таких технічних заходів, якщо вони можуть іншим чином забезпечити можливість реагування на запит відповідно до статті 15 протягом терміну, передбаченого статтею 12(3).

- Стаття 11(2) GDPR, контролер не може ідентифікувати суб'єкта даних

95. Якщо у відеозаписі немає можливості пошуку персональних даних (тобто контролеру, ймовірно, доведеться переглянути велику кількість збережених матеріалів, щоб знайти відповідного суб'єкта даних), контролер може бути не в змозі ідентифікувати суб'єкта даних.

96. Із цих причин суб'єкт даних повинен (окрім ідентифікації себе, в тому числі за допомогою документа, що посвідчує особу, або особисто) у своєму запиті до контролера вказати, коли — протягом обґрунтованого періоду часу, пропорційного до кількості зареєстрованих суб'єктів даних, — він увійшов у зону моніторингу. Контролер повинен заздалегідь повідомити суб'єкта даних про те, яка інформація необхідна для виконання запиту. Якщо контролер може довести, що він не в змозі ідентифікувати суб'єкта даних, він повинен поінформувати про це суб'єкта

даних, якщо це можливо. У такій ситуації у своїй відповіді суб'єкту даних контролер повинен повідомити про точну територію для моніторингу, перевірку камер, які використовувалися тощо, щоб суб'єкт даних мав повне розуміння того, які його персональні дані могли бути оброблені.

Приклад: Якщо суб'єкт даних запитує копію своїх персональних даних, оброблених за допомогою відеоспостереження на вході до торгового центру з-понад 30 000 відвідувачів на день, суб'єкт даних повинен вказати, коли він проходив зону спостереження в межах приблизно годинного часового проміжку. Якщо контролер все ще обробляє матеріал, необхідно надати копію відеозапису. Якщо в тому самому матеріалі можна ідентифікувати інших суб'єктів даних, то ця частина матеріалу повинна бути знеособлена (наприклад, шляхом розмиття копії або її частин), перш ніж надавати копію суб'єкту даних, який подав запит.

Приклад: Якщо контролер автоматично видаляє весь відзнятий матеріал, наприклад, протягом 2 днів, контролер не може надати відзнятий матеріал суб'єкту даних після закінчення цих 2 днів. Якщо контролер отримує запит після цих 2 днів, суб'єкт даних повинен бути відповідним чином проінформований.

97.

- Стаття 12 GDPR, надмірні запити

98. У разі надмірних або явно необґрунтованих запитів від суб'єкта даних контролер може або стягувати обґрунтовану плату відповідно до статті 12(5)(a) GDPR, або відмовити у виконанні запиту (стаття 12(5)(b) GDPR). Контролер повинен довести явно необґрунтований або надмірний характер запиту.

6.2 Право на видалення та право на заперечення

6.2.1 Право на видалення (право на забуття)

99. Якщо контролер продовжує обробку персональних даних поза межами моніторингу в режимі реального часу (наприклад, зберігання), суб'єкт даних може вимагати видалення персональних даних відповідно до статті 17 GDPR.

100. За запитом контролер зобов'язаний видалити персональні дані без будь-якої безпідставної затримки, якщо застосовується одна з обставин, перелічених у статті 17(1) GDPR (і жоден з винятків, перелічених у статті 17(3) GDPR, не застосовується). Це включає обов'язок видаляти персональні дані, коли вони більше не потрібні для цілей, для яких вони спочатку зберігалися, або коли обробка є незаконною (див. також *розділ 8 «Терміни зберігання та зобов'язання щодо видалення»*). Крім того, залежно від законної підстави обробки, персональні дані мають бути видалені:

- на підставі *згоди*, якщо згоду відкликано (та немає іншої законної підстави для обробки);
- на підставі *законного інтересу:*

Прийнято

- коли суб’єкт даних користується правом на заперечення (див. *розділ 6(2)(2)*) і немає більш вагомих законних підстав для обробки, або
- у випадку прямого маркетингу (включаючи профайлінг), коли суб’єкт даних заперечує проти обробки.

101. Якщо контролер оприлюднив відеозапис (наприклад, шляхом трансляції або потокової передачі в Інтернеті), необхідно вжити відповідних заходів для інформування інших контролерів (які наразі обробляють відповідні персональні дані) про запит згідно зі статтею 17(2) GDPR. Відповідні заходи мають включати технічні заходи, враховуючи наявні технології та витрати на їхню реалізацію. Наскільки це можливо, контролер повинен повідомити — після видалення персональних даних — усіх, кому раніше були розкриті персональні дані, відповідно до статті 19 GDPR.

102. Окрім обов’язку контролера видаляти персональні дані на вимогу суб’єкта даних, контролер зобов’язаний відповідно до загальних принципів GDPR обмежити обсяг персональних даних, що зберігаються (див. *розділ 8*).

103. У випадку відеоспостереження варто зазначити, що, наприклад, у разі розмиття зображення без можливості ретроактивного відновлення персональних даних, які раніше містилися на зображенні, персональні дані вважаються видаленими відповідно до GDPR.

> Приклад: Магазин має проблеми з вандалізмом, зокрема, на своїй зовнішній стороні, і тому використовує відеоспостереження за межами свого входу, безпосередньо розташованого біля стін. Перехожий звертається з проханням видалити його персональні дані із цього самого моменту. Контролер зобов’язаний відповісти на запит без невиправданої затримки й не пізніше, ніж протягом одного місяця. Оскільки відеозапис, про який йде мова, більше не відповідає меті, з якою він спочатку зберігався (за час, поки суб’єкт даних проходив повз нього, не відбулося жодних актів вандалізму), на момент запиту не існує законного інтересу зберігати ці дані, який би переважав над інтересами суб’єктів даних. Контролер повинен видалити персональні дані.

104.

6.2.2 Право на заперечення

105. У випадку відеоспостереження на підставі *законних інтересів* (стаття 6(1)(f) GDPR) або необхідності виконання завдання в *суспільних інтересах* (стаття 6(1)(e) GDPR) суб’єкт даних має право в будь-який час заперечити проти обробки на підставах, пов’язаних з його конкретною ситуацією, відповідно до статті 21 GDPR. Якщо контролер не доведе вагомі законні підстави, які переважають над правами та інтересами суб’єкта даних, обробка даних особи, яка заперечує, має бути припинена. Контролер зобов’язаний відповідати на запити суб’єкта даних без невиправданої затримки й не пізніше, ніж протягом одного місяця.

Прийнято

106. У контексті відеоспостереження таке заперечення може бути зроблене або при вході, або під час перебування в зоні спостереження, або після виходу з неї. На практиці це означає, що якщо контролер не має вагомих законних підстав, моніторинг території, на якій можна ідентифікувати фізичну особу, є законним, лише якщо:

(1) контролер має можливість негайно зупинити обробку камерою персональних даних за запитом, або

(2) зона моніторингу настільки детально обмежена, що контролер може отримати дозвіл від суб'єкта даних до входу в цю зону, і вона не є зоною, до якої суб'єкт даних як громадянин має право доступу.

107. Ці настанови не мають на меті визначити, що вважається *вагомим* законним інтересом (стаття 21 GDPR).

108. При використанні відеоспостереження для цілей прямого маркетингу суб'єкт даних має право заперечувати проти обробки на власний розсуд, оскільки право на заперечення в цьому контексті є абсолютним (пункти 2 і 3 статті 21 GDPR).

> Приклад: Компанія відчуває труднощі з порушенням безпеки на своєму громадському вході та використовує відеоспостереження на підставі законного інтересу з метою виявлення осіб, які незаконно проникають на територію. Відвідувач заперечує проти обробки його даних через систему відеоспостереження на підставах, що стосуються його конкретної ситуації. Однак у цьому випадку компанія відхиляє запит з поясненням, що збережені відеозаписи необхідні для проведення внутрішнього розслідування, а отже, має вагомі законні підстави для продовження обробки персональних даних.

109.

Прийнято

7 ЗОБОВ'ЯЗАННЯ ЩОДО ПРОЗОРОСТІ ІНФОРМАЦІЇ[18]

110. Європейське законодавство про захист даних вже давно передбачає, що суб'єкти даних повинні знати про те, що ведеться відеоспостереження. Вони повинні бути детально поінформовані про місця, за якими ведеться спостереження.[19] Відповідно до GDPR, загальні зобов'язання щодо прозорості інформації викладені в статті 12 GDPR та наступних статтях. «Настанови щодо прозорості відповідно до Регламенту 2016/679 (РД 260)», розроблені Робочою групою за статтею 29, які були схвалені EDPB 25 травня 2018 року, надають більш детальну інформацію. Відповідно до РД 260, п. 26, саме стаття 13 GDPR застосовується, якщо персональні дані збираються «[...] від суб'єкта даних шляхом спостереження (наприклад, за допомогою автоматизованих пристроїв збору даних або програмного забезпечення для збору даних, таких як камери [...]».

111. З огляду на обсяг інформації, яку необхідно надати суб'єкту даних, контролери даних можуть застосовувати багаторівневий підхід, коли вони вирішують використовувати комбінацію методів для забезпечення прозорості (РД 260, п. 35; РД 89, п. 22). Що стосується відеоспостереження, то найважливіша інформація повинна відображатися на самому попереджувальному знаку (перший рівень), тоді як подальші обов'язкові деталі можуть бути надані іншими засобами (другий рівень).

7.1 Інформація першого рівня (попереджувальний знак)

112. Перший рівень стосується основного способу, в який контролер вперше взаємодіє із суб'єктом даних. На цьому етапі контролери можуть використовувати попереджувальний знак, що відображає відповідну інформацію. Інформація, що відображається, може надаватися у поєднанні стандартизованими іконками для того, щоб надати конструктивний огляд призначеної обробки у видимий, доступний для розуміння та чіткий спосіб (стаття 12(7) GDPR). Формат інформації має бути адаптований до конкретного місця розташування (РД 89, п. 22).

7.1.1 Розміщення попереджувального знаку

113. Інформація має бути розміщена таким чином, щоб суб'єкт даних міг легко розпізнати обставини спостереження до того, як він увійде в зону спостереження (приблизно на рівні очей). Не обов'язково показувати розташування камери, якщо немає сумнівів щодо того, які зони

[18] Можуть застосовуватися конкретні вимоги національного законодавства.

[19] РД 89, Висновок 4/2004 про обробки персональних даних за допомогою відеоспостереження Робочої групи за статтею 29.

Прийнято

підлягають спостереженню, і контекст спостереження однозначно з'ясований (РД 89, п. 22). Суб'єкт даних повинен мати можливість оцінити, яку саме ділянку охоплює камера, щоб мати змогу уникнути спостереження або змінити свою поведінку, якщо це необхідно.

7.1.2 Зміст першого рівня

114. Інформація першого рівня (попереджувальний знак), як правило, повинна передавати найважливішу інформацію, наприклад, деталі цілей обробки, ідентифікацію контролера та існування прав суб'єкта даних, а також інформацію про найбільші наслідки обробки.[20] Це може включати, зокрема, законні інтереси, які переслідує контролер (або третя сторона), а також контактні дані відповідального за захист даних (якщо це можливо). Він також повинен містити посилання на більш детальний другий рівень інформації, а також на те, де і як його можна знайти.

115. Крім того, попереджувальний знак повинен містити будь-яку інформацію, яка може бути новою для суб'єкта даних (РД 260, п. 38). Це може бути, наприклад, передача даних третім особам, особливо якщо вони знаходяться за межами ЄС, а також термін зберігання. Якщо ця інформація не вказана, суб'єкт даних має можливість довіряти тому, що ведеться виключно моніторинг у режимі реального часу (без запису або передачі даних третім особам).

[20] Див. РД 260, п. 38.

116.

Приклад (необов'язкова рекомендація):

Увага! Ведеться відеоспостереження!

Більш детальна інформація доступна:
- через повідомлення
- на рецепції/інформація для клієнтів/реєстрація
- через інтернет (URL)...

Ідентифікаційні дані контролера та, за необхідності, представника контролера:

Контактні дані, в тому числі особи, відповідальної за захист даних (якщо це можливо):

Інформація про обробку, яка має найбільший вплив на суб'єкта даних (наприклад, період зберігання або спостереження у режимі реального часу, публікація або передача відеоматеріалів третім особам):

Цілі відеоспостереження:

Права суб'єктів даних: Як суб'єкт даних ви маєте кілька прав, зокрема право вимагати від контролера доступу до ваших персональних даних або їх видалення.

Для отримання детальної інформації про це відеоспостереження, включаючи ваші права, ознайомтеся з повною інформацією, наданою контролером за допомогою опцій, представлених зліва.

7.2 Інформація другого рівня

117. Інформація другого рівня також повинна бути доступна в місці, зручному для суб'єкта даних, зокрема у вигляді повного інформаційного бюлетеня, розміщеного в центральному місці (наприклад, на інформаційній стійці, в приймальні або на касі), або на зручному для ознайомлення плакаті. Як зазначалося вище, попереджувальний знак першого рівня повинен чітко посилатися на інформацію другого рівня. Крім того, найкраще, якщо інформація першого рівня посилається на цифрове джерело (наприклад, QR-код або адресу вебсайту) другого рівня. Однак інформація також повинна бути легко доступною в нецифровому вигляді. Має бути можливість отримати доступ до інформації другого рівня без відвідування території, за якою ведеться спостереження, особливо якщо інформація надається в цифровому вигляді (цього можна досягти, наприклад, за допомогою посилання). Іншим відповідним засобом може бути номер телефону, за яким можна зателефонувати. Незалежно від того, яким чином надається інформація, вона повинна містити все, що є обов'язковим відповідно до статті 13 GDPR.

118. На додаток до цих варіантів, а також для того, щоб зробити їх більш ефективними, EDPB заохочує використання технічних засобів для надання інформації суб'єктам даних. Це може включати, зокрема, геолокацію камер і включення інформації в картографічні додатки або вебсайти, щоб особи могли легко, з одного боку, ідентифікувати та вказати джерела відео, пов'язані з реалізацією їхніх прав, а з іншого боку, отримати більш детальну інформацію про операцію з обробки.

Прийнято

Приклад: Власник магазину веде спостереження свого магазину. Для дотримання вимог статті 13 йому достатньо розмістити попереджувальний знак на видному місці біля входу в магазин, який містить інформацію першого рівня. Крім того, він повинен надати інформаційний листок, що містить інформацію другого рівня, на касі або в будь-якому іншому центральному та доступному місці у своєму магазині.

119.

8 ТЕРМІНИ ЗБЕРІГАННЯ ТА ЗОБОВ'ЯЗАННЯ ЩОДО ВИДАЛЕННЯ

120. Персональні дані не можуть зберігатися довше, ніж це необхідно для цілей, для яких здійснюється обробка персональних даних (стаття 5(1)(c) і (e) GDPR). У деяких державах-членах можуть існувати окремі положення щодо термінів зберігання даних відеоспостереження відповідно до статті 6(2) GDPR.

121. Необхідність зберігання персональних даних повинна контролюватися у вузьких часових рамках. Загалом, законними цілями відеоспостереження часто є захист майна або збереження доказів. Зазвичай збитки, що виникли, можуть бути визнані протягом одного-двох днів. Щоб полегшити доведення дотримання вимог законодавства про захист даних, в інтересах контролера заздалегідь вжити організаційних заходів (наприклад, призначити, за необхідності, представника для перегляду та збереження відеоматеріалів). Беручи до уваги принципи статті 5(1)(c) та (e) GDPR, а саме мінімізацію даних та обмеження терміну зберігання, персональні дані в більшості випадків (наприклад, з метою виявлення актів вандалізму) повинні бути видалені, в ідеалі автоматично, через кілька днів. Чим довший встановлений термін зберігання (особливо якщо він перевищує 72 години), тим більше аргументації має бути надано для обґрунтування законності мети та необхідності зберігання. Якщо контролер використовує відеоспостереження не лише для моніторингу своїх приміщень, але й має намір зберігати дані, він повинен переконатися, що зберігання дійсно необхідне для досягнення поставленої мети. Якщо це так, період зберігання повинен бути чітко визначений і встановлений індивідуально для кожної конкретної мети. Контролер несе відповідальність за визначення періоду зберігання відповідно до принципів необхідності та пропорційності, а також за доведення відповідності положенням GDPR.

Приклад: Власник невеликого магазину зазвичай помічає будь-який акт вандалізму того ж дня. Як наслідок, звичайний період зберігання 24 години є достатнім. Однак закриття протягом вихідних або тривалих свят може стати причиною для більш тривалого періоду зберігання. Якщо буде виявлено пошкодження, йому також може знадобитися зберігати відеозапис довше, щоб вжити правових заходів проти правопорушника.

122.

Прийнято

9 ТЕХНІЧНІ ТА ОРГАНІЗАЦІЙНІ ЗАХОДИ

123. Як зазначено в статті 32(1) GDPR, обробка персональних даних під час відеоспостереження має бути не лише дозволена законом, але й належним чином захищена контролерами та операторами. Впроваджувані **організаційні та технічні заходи** повинні бути **пропорційними ризикам для прав і свобод фізичних осіб**, що виникають внаслідок випадкового або незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до даних відеоспостереження. Згідно зі статтями 24 і 25 GDPR, контролери повинні впроваджувати технічні та організаційні заходи також для того, щоб забезпечити дотримання всіх принципів захисту даних під час обробки, а також створити засоби для реалізації суб'єктами даних своїх прав, визначених у статтях 15-22 GDPR. Контролери даних повинні прийняти внутрішні рамки та політику, які забезпечують цю реалізацію як під час визначення засобів для обробки, так і під час самої обробки, включаючи оцінку впливу на захист даних, коли це необхідно.

9.1 Огляд системи відеоспостереження

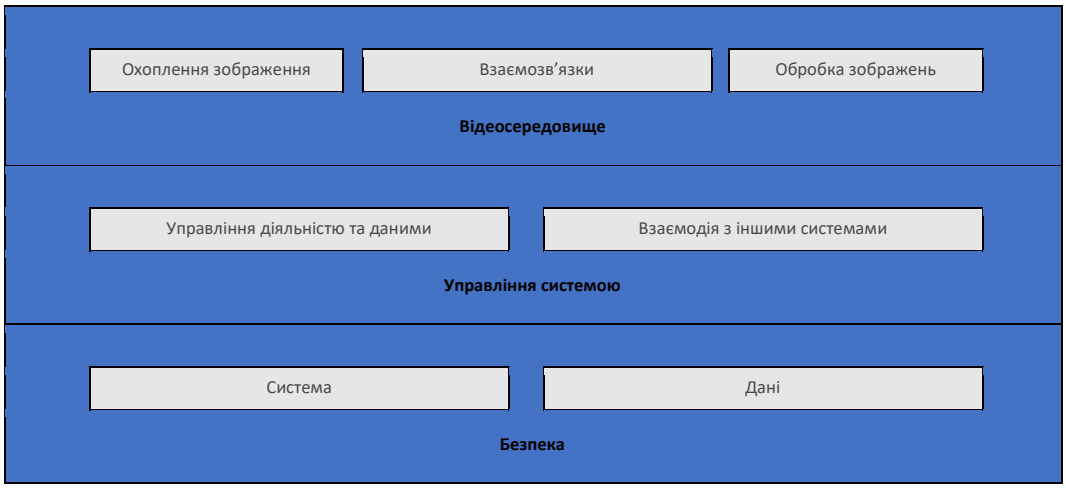
124. Система відеоспостереження (СВС)[21] складається з аналогових і цифрових пристроїв, а також програмного забезпечення, призначених для охоплення зображень території, обробки зображень і відображення їх оператору. Її компоненти згруповані в такі категорії:

- Відеосередовище: охоплення зображень, взаємозв'язок та обробка зображень:
  - метою охоплення зображення є створення зображення реального світу в такому форматі, щоб воно могло бути використане рештою системи;
  - взаємозв'язки описують всю передачу даних у відеосередовищі, тобто з'єднання та комунікації. Прикладами з'єднань є кабелі, цифрові мережі та бездротова передача даних. Комунікації описують усі відеосигнали та сигнали керування, які можуть бути цифровими або аналоговими;
  - обробка зображень включає аналіз, зберігання та представлення зображення або послідовності зображень.
- З точки зору управління системою, СВС виконує такі логічні функції:
  - управління даними та діяльністю, що включає обробку команд оператора та системних дій (процедури сигналізації, оповіщення операторів);

[21] GDPR не дає визначення цього поняття, технічний опис можна знайти, зокрема, у стандарті EN 62676-1-1:2014 «Системи відеоспостереження охоронного призначення. Частина 1-1: Вимоги до відеосистем».
Прийнято

- інтерфейси з іншими системами можуть включати підключення до інших охоронних (контроль доступу, пожежна сигналізація) і неохоронних систем (системи управління будівлею, автоматичне розпізнавання номерних знаків).

- Безпека СВС передбачає конфіденційність, цілісність та доступність системи й даних:
  - безпека системи включає фізичну безпеку всіх компонентів системи та контроль доступу до СВС;
  - безпека даних включає запобігання втраті або маніпулюванню даними.



125.

Рисунок 1 - Система відеоспостереження

9.2 Захист даних за призначенням і за замовчуванням

126. Як зазначено в статті 25 GDPR, контролери повинні, у момент визначення засобів обробки та в момент самої обробки відеоматеріалів, вжити необхідних технічних та організаційних заходів щодо захисту даних. Ці принципи підкреслюють необхідність використання вбудованих технологій, що підвищують конфіденційність, налаштувань за замовчуванням, які мінімізують обробку даних, а також надання необхідних інструментів, які забезпечують максимально можливий захист персональних даних[22].

127. Контролери повинні вбудовувати захист даних і гарантії конфіденційності не лише в проектні специфікації технології, але й в організаційну практику. Що стосується організаційних практик, то

[22] РД 168. Висновок про «майбутнє конфіденційності», спільний внесок Робочої групи з питань захисту даних за статтею 29 та Робочої групи з питань правоохоронних органів та правосуддя до консультацій Європейської Комісії щодо правових рамок основоположного права на захист персональних даних (прийнятий 01 грудня 2009 року).
Прийнято

контролер повинен прийняти відповідну систему управління, розробити та впровадити політику та процедури, пов'язані з відеоспостереженням. З технічної точки зору, специфікація та проектування системи повинні включати вимоги щодо обробки персональних даних відповідно до принципів, викладених у статті 5 GDPR (законність оброки, мета та обмеження даних, мінімізація даних за замовчуванням у розумінні статті 25(2) GDPR, цілісність та конфіденційність, підзвітність тощо). Якщо контролер планує придбати комерційну систему відеоспостереження, він повинен включити ці вимоги до специфікації закупівлі. Контролер повинен забезпечити дотримання цих вимог, застосовуючи їх до всіх компонентів системи та до всіх даних, які вона обробляє, протягом усього їхнього життєвого циклу.

9.3 Конкретні приклади відповідних заходів

128. Більшість заходів, які можна застосувати для захисту відеоспостереження, особливо якщо використовується цифрове обладнання та програмне забезпечення, не будуть відрізнятися від тих, що застосовуються в інших IT-системах. Однак, незалежно від обраного рішення, контролер повинен належним чином захищати всі компоненти системи відеоспостереження й дані на всіх етапах, тобто під час зберігання (дані в стані спокою), передачі (дані під час передачі) та обробки (дані в процесі використання). Для цього необхідно, щоб контролери та оператори поєднували організаційні та технічні заходи.

129. При виборі технічних рішень контролер повинен враховувати технології, що не порушують конфіденційність, ще й тому, що вони підвищують безпеку. Прикладами таких технологій є системи, які дозволяють маскувати або кодувати ділянки, що не мають відношення до спостереження, або видаляти зображення третіх осіб при наданні відеоматеріалів суб'єктам даних.[23] З іншого боку, обрані рішення не повинні забезпечувати функції, які не є необхідними (наприклад, необмежене переміщення камер, можливість масштабування, радіопередачу, аналіз та аудіозаписи). Функції, які надаються, але не є необхідними, повинні бути деактивовані.

130. Існує багато літератури на цю тему, включаючи міжнародні стандарти й технічні специфікації щодо фізичної безпеки мультимедійних систем[24], а також безпеки загальних IT-систем[25]. Тому цей розділ містить лише загальний огляд даної теми.

[23] Використання таких технологій може бути навіть обов'язковим у деяких випадках для дотримання вимог статті 5(1)(c). У будь-якому випадку вони можуть слугувати прикладами найкращих практик.

[24] IEC TS 62045 - Безпека мультимедіа - Настанова щодо захисту конфіденційності обладнання та систем під час використання та поза ним.

[25] ISO/IEC 27000 - Системи управління інформаційною безпекою.

Прийнято

9.3.1 Організаційні заходи

131. Окрім потенційно необхідної оцінки впливу на захист даних (див. *розділ 10*), при розробленні власної політики та процедур відеоспостереження контролери повинні розглянути такі питання:

- Хто відповідає за управління та експлуатацію системи відеоспостереження.
- Мета та обсяг проекту відеоспостереження.
- Належне та заборонене використання (де і коли відеоспостереження дозволено, а де і коли — ні; наприклад, використання прихованих камер та аудіозаписів на додаток до відеозапису)[26].
- Заходи забезпечення прозорості, про які йдеться в *розділі 7 (Зобов'язання щодо прозорості інформації).*
- Як ведеться відеозапис і протягом якого часу, включаючи архівне зберігання відеозаписів, пов'язаних з інцидентами, що стосуються безпеки.
- Хто і коли повинен пройти відповідне навчання.
- Хто має доступ до відеозаписів і з якою метою.
- Операційні процедури (наприклад, хто і звідки здійснює моніторинг відеоспостереження, що робити у випадку порушення безпеки даних).
- Процедури, яких повинні дотримуватися зовнішні сторони, щоб отримати відеозаписи, а також процедури відхилення або задоволення таких запитів.
- Процедури закупівлі, встановлення та обслуговування СВС.
- Процедури управління інцидентами та відновлення.

9.3.2 Технічні заходи

132. **Безпека системи** означає **фізичну безпеку** всіх компонентів системи, а також цілісність системи, тобто **захист від навмисного та ненавмисного втручання в її нормальне функціонування та контроль доступу**, та **її стійкість до таких втручань**. Безпека даних означає **конфіденційність** (доступ до даних мають лише ті, кому надано доступ), **цілісність** (запобігання втраті даних або маніпуляціям з ними) та **доступність** (доступ до даних можливий тоді, коли вони потрібні).

133. **Фізична безпека** є життєво важливою частиною захисту даних і першою лінією оборони, оскільки вона захищає обладнання СВС від крадіжок, вандалізму, стихійних лих, техногенних катастроф і випадкових пошкоджень (зокрема від перепадів напруги, екстремальних температур і розлитої кави). У випадку аналогових систем фізична безпека відіграє головну роль у їхньому захисті.

[26] Це може залежати від національного законодавства та галузевих норм.

134. **Безпека системи та даних**, тобто захист від навмисного та ненавмисного втручання в її нормальне функціонування, може включати:

- захист всієї інфраструктури СВС (включаючи віддалені камери, кабелі та джерела живлення) від фізичного втручання та крадіжки;
- захист передачі відзнятого матеріалу за допомогою захищених від перехоплення каналів зв'язку;
- шифрування даних;
- використання апаратних і програмних рішень, таких як брандмауери, антивіруси або системи виявлення вторгнень, для захисту від кібератак;
- виявлення збоїв компонентів, програмного забезпечення та з'єднань;
- засоби відновлення працездатності та доступу до системи в разі фізичного або технічного інциденту.

135. **Контроль доступу** гарантує, що тільки уповноважені особи можуть отримати доступ до системи й даних, на відміну від інших осіб, які не мають такої можливості. Заходи, які підтримують фізичний і логічний контроль доступу, включають:

- забезпечення того, щоб усі приміщення, де здійснюється моніторинг за допомогою відеоспостереження і де зберігаються відеозаписи, були захищені від несанкціонованого доступу третіх осіб;
- розміщення моніторів таким чином (особливо якщо вони знаходяться у відкритих приміщеннях, наприклад, у приймальні), щоб їх могли бачити лише уповноважені оператори;
- визначення та застосування процедур надання, зміни та відкликання фізичного й логічного доступу;
- впровадження методів та засобів автентифікації та авторизації користувачів, включаючи, зокрема, довжину паролів та частоту їх зміни;
- реєстрацію та регулярний перегляд дій користувачів (як із системою, так і з даними);
- здійснення безперервного моніторингу та виявлення збоїв у доступі, а також усунення недоліків у найкоротші терміни.

10 ОЦІНКА ВПЛИВУ НА ЗАХИСТ ДАНИХ

136. Відповідно до статті 35(1) GDPR контролери зобов'язані проводити оцінку впливу на захист даних (DPIA), коли тип обробки даних може призвести до високого ризику для прав і свобод фізичних осіб. Стаття 35(3)(c) GDPR передбачає, що контролери зобов'язані проводити оцінку впливу на захист даних, якщо обробка являє собою систематичний та широкомасштабний моніторинг зони, що знаходиться у відкритому доступі. Крім того, відповідно до статті 35(3)(b) GDPR, оцінка впливу на захист даних також необхідна, коли контролер має намір здійснити широкомасштабну обробку спеціальних категорій даних.

Прийнято

137. Настанови щодо оцінки впливу на захист даних[27] надають подальші поради та більш детальні приклади, що стосуються відеоспостереження (наприклад, щодо «використання системи камер для моніторингу поведінки водіїв на автомагістралях»). Стаття 35(4) GDPR вимагає, щоб кожен наглядовий орган опублікував перелік операцій з обробки даних, які підлягають обов'язковій оцінці впливу на захист даних у своїй країні. Ці переліки зазвичай можна знайти на вебсайтах органів влади. З огляду на типові цілі відеоспостереження (захист людей і майна, виявлення, запобігання та контроль правопорушень, збір доказів і біометрична ідентифікація підозрюваних), обґрунтовано припустити, що в багатьох випадках відеоспостереження вимагатиме оцінки впливу на захист даних. Тому контролерам даних слід уважно ознайомитися із цими документами, щоб визначити, чи потрібна така оцінка, і провести її в разі необхідності. Результати проведеної оцінки впливу на захист даних повинні визначати вибір контролером заходів захисту даних, які він буде впроваджувати.

138. Важливо також зазначити, що якщо результати оцінки впливу на захист даних вказують на те, що обробка може призвести до високого ризику, попри заходи безпеки, заплановані контролером, то необхідно буде проконсультуватися з відповідним наглядовим органом перед початком обробки. Детальну інформацію про попередні консультації можна знайти в статті 36.

Від імені Європейської ради із захисту даних

Голова

(Андреа Єлінек)

[27] РД 248, версія 01. Настанови щодо оцінки впливу на захист даних (DPIA) та визначення того, чи обробка «може призвести до високого ризику» для цілей Регламенту 2016/679. – схвалені EDPB
Прийнято