Настанови

Настанови 4/2019 щодо статті 25

Захист даних за призначенням і за замовчуванням

Версія 2.0

Прийнято 20 жовтня 2020 року

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

Історія версій

Версія 1.0	13 листопада 2019 року	Прийняття Настанов для публічних консультацій
Версія 2.0	20 жовтня 2020 року	Ухвалення Настанов EDPB після публічних консультацій

Прийнято

Зміст

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,

Беручи до уваги статтю 12 та статтю 22 його Регламенту,

ПРИЙНЯЛА ТАКІ НАСТАНОВИ

Короткий огляд

У світі, який стає все більш цифровим, дотримання вимог щодо захисту даних за призначенням і за замовчуванням відіграє вирішальну роль у забезпеченні конфіденційності та захисту даних у суспільстві. Тому важливо, щоб контролери серйозно ставилися до цієї відповідальності та виконували зобов'язання GDPR при розробленні операцій з обробки даних.

Ці Настанови надають загальні вказівки щодо зобов'язання із захисту даних за призначенням і за замовчуванням («DPbDD»), викладеного в статті 25 GDPR. Захист даних за призначенням і за замовчуванням є зобов'язанням для всіх контролерів, незалежно від розміру та різної складності обробки. Для того, щоб мати можливість виконувати вимоги із захисту даних за призначенням і за замовчуванням, важливо, щоб контролер розумів принципи захисту даних, а також права й свободи суб'єкта даних.

Основним зобов'язанням є впровадження *відповідних* заходів та необхідних гарантій, які забезпечують *ефективну реалізацію принципів захисту даних* і, відповідно, *прав і свобод суб'єктів даних за призначенням і за замовчуванням.* Стаття 25 визначає елементи, які слід брати до уваги як за призначенням, так і за замовчуванням. Ці елементи будуть більш детально розглянуті в цих Настановах.

Стаття 25(1) передбачає, що контролери повинні враховувати принципи захисту даних за призначенням і за замовчуванням на ранніх етапах планування нової операції з обробки даних. Контролери повинні впроваджувати принципи захисту даних за призначенням і за замовчуванням *до початку* обробки, а також *постійно* під час процесу обробки, регулярно переглядаючи ефективність обраних заходів та гарантій. Принципи захисту даних за призначенням і за замовчуванням також застосовуються до існуючих систем, які обробляють персональні дані.

Настанови також містять вказівки щодо ефективного впровадження принципів захисту даних, викладених у статті 5, з переліком ключових елементів за призначенням і за замовчуванням, а також практичних кейсів для ілюстрації. Контролер повинен розглянути доцільність запропонованих заходів у контексті конкретної обробки, про яку йдеться.

Прийнято

EDPB надає рекомендації щодо того, як контролери, оператори та виробники можуть співпрацювати для забезпечення захисту даних за призначенням і за замовчуванням. Вона заохочує контролерів у промисловості, операторів та виробників використовувати принципи захисту даних за призначенням і за замовчуванням як засіб досягнення конкурентної переваги при просуванні своєї продукції на ринку контролерам та суб'єктам даних. Вона також заохочує всіх контролерів використовувати сертифікацію та кодекси поведінки.

Прийнято

1 СФЕРА ЗАСТОСУВАННЯ

1. Настанови зосереджені на впровадженні контролерами принципів захисту даних за призначенням і за замовчуванням на основі зобов'язань, передбачених статтею 25 GDPR.[1] Інші суб'єкти, такі як оператори та виробники продуктів, послуг і додатків (далі — «виробники»), які безпосередньо не згадуються в статті 25, також можуть знайти ці Настанови корисними для створення сумісних із GDPR продуктів і послуг, які дозволять контролерам виконувати свої зобов'язання щодо захисту даних.[2] У преамбулі 78 GDPR додається, що принципи захисту даних за призначенням і за замовчуванням необхідно брати до уваги в контексті публічних тендерів. Попри те, що всі контролери зобов'язані інтегрувати принципи захисту даних за призначенням і за замовчуванням у свою діяльність з обробки даних, це положення сприяє прийняттю принципів захисту даних, де державні адміністрації повинні показувати приклад. Контролер несе відповідальність за виконання зобов'язань із захисту даних за призначенням і за замовчуванням щодо обробки, яке здійснюють його оператори та субоператори, тому він повинен враховувати це при укладанні договорів із цими сторонами.

2. Вимога, описана в статті 25, полягає в тому, що контролери повинні передбачити захист даних при обробці персональних даних за замовчуванням, і це застосовується протягом усього життєвого циклу обробки. Принципи захисту даних за призначенням і за замовчуванням також є вимогою для систем обробки, що існували до набрання чинності GDPR. Контролери повинні постійно оновлювати обробку даних відповідно до GDPR. Для отримання додаткової інформації про те, як підтримувати існуючу систему відповідно до принципів захисту даних за призначенням і за замовчуванням, див. підпункт 2.1.4 цих Настанов. Суть цього положення полягає в забезпеченні *належного* та *ефективного* захисту даних як *за призначенням*, так і *за замовчуванням*, а це означає, що контролери мають можливість довести, що вони вживають відповідних заходів і гарантій у процесі обробки, щоб забезпечити дотримання принципів захисту даних, а також прав і свобод суб'єктів даних.

3. Глава 2 Настанов зосереджена на тлумаченні вимог, викладених у статті 25, та досліджує юридичні зобов'язання, що накладаються цим положенням. Приклади застосування принципів захисту даних за призначенням і за замовчуванням у контексті конкретних принципів захисту даних наведені у главі 3.

4. У главі 4 Настанов розглядається можливість створення механізму сертифікації для доведення відповідності статті 25, а також те, як наглядові органи можуть застосовувати цю статтю у главі 5.

---

[1] Наведені тут тлумачення однаково стосуються статті 20 Директиви (ЄС) 2016/680 та статті 27 Регламенту 2018/1725.

[2] Преамбула 78 GDPR чітко вказує на цю необхідність: *«При розробленні, проектуванні, виборі та використанні додатків, послуг і продуктів, які базуються на обробці персональних даних або обробляють персональні дані для виконання своїх завдань, слід заохочувати виробників продуктів, послуг і додатків враховувати право на захист даних при розробленні та проектуванні таких продуктів, послуг і додатків, а також, з належним урахуванням «сучасного рівня розвитку», переконатися, що контролери та оператори здатні виконувати свої зобов'язання щодо захисту даних».*
Прийнято

Зрештою, Настанови надають зацікавленим сторонам додаткові рекомендації щодо того, як успішно впроваджувати принципи захисту даних за призначенням і за замовчуванням. EDPB визнає, що малим та середнім підприємствам (далі — «МСП») складно повністю виконати зобов'язання щодо захисту даних за призначенням і за замовчуванням, і надає додаткові рекомендації спеціально для МСП у главі 6.

2 АНАЛІЗ СТАТТІ 25(1) ТА (2) «ЗАХИСТ ДАНИХ ЗА ПРИЗНАЧЕННЯМ І ЗА ЗАМОВЧУВАННЯМ»

5. Метою цієї глави є вивчення та надання рекомендацій щодо вимог до захисту даних за призначенням у статті 25(1) та до захисту даних за замовчуванням у статті 25(2), відповідно. Захист даних за призначенням і захист даних за замовчуванням є взаємодоповнюючими концепціями, які взаємно підсилюють одна одну. Суб'єкти даних отримають більше переваг від захисту даних за замовчуванням, якщо паралельно буде впроваджено захист даних за призначенням, і навпаки.

6. Захист даних за призначенням і за замовчуванням є вимогою для всіх контролерів, включаючи малі підприємства та транснаціональні компанії. З огляду на це, складність впровадження принципів захисту даних за призначенням і за замовчуванням може варіюватися залежно від окремої операції з обробки. Однак, незалежно від розміру, у всіх випадках впровадження принципів захисту даних за призначенням і за замовчуванням може принести позитивні переваги як контролеру, так і суб'єкту даних.

2.1 Стаття 25(1): Захист даних за призначенням

2.1.1 Зобов'язання контролера впроваджувати відповідні технічні та організаційні заходи та необхідні гарантії в процесі обробки

7. Згідно зі статтею 25(1), контролер зобов'язаний вжити *відповідних* технічних та організаційних *заходів*, спрямованих на реалізацію принципів захисту даних та інтеграцію *необхідних гарантій* у процес обробки з метою дотримання вимог та захисту прав і свобод суб'єктів персональних даних. Як відповідні заходи, так і необхідні гарантії повинні служити одній меті — захисту прав суб'єктів даних та забезпеченню того, щоб захист їхніх персональних даних був вбудований у процес обробки.

8. *Технічні й організаційні заходи* та необхідні *гарантії* можна розуміти в широкому сенсі як будь-який метод або засіб, який контролер може використовувати в процесі обробки. *Відповідність* означає, що заходи та необхідні гарантії повинні бути придатними для досягнення поставленої мети, тобто вони повинні *ефективно*[3] реалізовувати принципи захисту даних. Таким чином, вимога щодо відповідності тісно пов'язана з вимогою ефективності.

9. Технічними або організаційними заходами та гарантіями можуть бути будь-які дії — від використання передових технічних рішень до базової підготовки персоналу. Приклади, які

[3] «Ефективність» розглядається нижче в підпункті 2.1.2.

можуть бути доцільними, залежно від контексту та ризиків, пов'язаних із відповідною обробкою, включають псевдонімізацію персональних даних [4] ; зберігання персональних даних у структурованому, загальнодоступному для машинного зчитування форматі; надання суб'єктам даних можливості втручатися в процес обробки; надання інформації про зберігання персональних даних; наявність систем виявлення шкідливого програмного забезпечення; навчання працівників основам «кібергігієни»; створення систем управління конфіденційністю та інформаційною безпекою; зобов'язання операторів на договірній основі впроваджувати конкретні практики мінімізації даних тощо.

10. Стандарти, найкращі практики та кодекси поведінки, визнані асоціаціями та іншими органами, що представляють категорії контролерів, можуть бути корисними при визначенні відповідних заходів. Однак контролер повинен перевірити доцільність заходів для конкретної обробки, про яку йдеться.

2.1.2 Розроблено для ефективного впровадження принципів захисту даних та захисту прав і свобод суб'єктів даних

11. *Принципи захисту даних* викладені в статті 5 (далі — «принципи»), *права та свободи суб'єктів даних* — це основоположні права та свободи фізичних осіб, зокрема, їхнє право на захист персональних даних, захист яких визначений у статті 1(2) як мета GDPR (далі — «права»)[5]. Їх точне формулювання можна знайти в Хартії основоположних прав ЄС. Важливо, щоб контролер розумів значення *принципів* і *прав* як основи для захисту, що пропонується GDPR, зокрема, зобов'язанням щодо захисту даних за призначенням і за замовчуванням.

12. При впровадженні відповідних технічних та організаційних заходів, саме з огляду на ефективну реалізацію кожного з вищезазначених принципів та подальший захист прав, мають бути *розроблені* заходи та гарантії.

Вирішення проблеми ефективності

13. Ефективність лежить в основі концепції захисту даних за призначенням. Вимога ефективної реалізації принципів означає, що контролери повинні вживати необхідних заходів і гарантій для захисту цих принципів з метою забезпечення прав суб'єктів даних. Кожен застосований захід повинен мати заплановані результати обробки, передбачені контролером. Це зауваження має два наслідки.

14. По-перше, це означає, що стаття 25 не вимагає впровадження будь-яких конкретних технічних та організаційних заходів, скоріше, обрані заходи та гарантії повинні бути специфічними для впровадження принципів захисту даних у конкретний процес обробки, про яку йдеться. При цьому заходи та гарантії мають бути розроблені таким чином, щоб бути надійними, а контролер повинен мати можливість вжити подальших заходів для того, щоб масштабувати їх до будь-якого

[4] Визначено в статті 4(5) GDPR.

[5] Див. преамбулу 4 GDPR.

збільшення ризику[6]. Таким чином, ефективність заходів залежатиме від контексту відповідної обробки та оцінки певних елементів, які слід враховувати при визначенні способу обробки. Вищезазначені елементи будуть розглянуті нижче в підпункті 2.1.3.

15. По-друге, контролери повинні довести, що ці принципи були дотримані.

16. Вжиті заходи та гарантії повинні досягати бажаного ефекту з точки зору захисту даних, а контролер повинен мати документацію про вжиті технічні та організаційні заходи.[7] Для цього контролер може визначити відповідні ключові показники ефективності (KPI), щоб продемонструвати ефективність. KPI — це обрана контролером вимірювана величина, яка демонструє, наскільки ефективно контролер досягає своєї мети щодо захисту даних. KPI можуть бути *кількісними*, наприклад, відсоток хибнопозитивних або хибнонегативних результатів, зменшення кількості скарг, скорочення часу відповіді, коли суб'єкти даних реалізують свої права; або *якісними*, наприклад, оцінка ефективності, використання шкал оцінювання або експертних оцінок. Як альтернативу KPI контролери можуть продемонструвати ефективну реалізацію принципів, надаючи обґрунтування своєї оцінки ефективності обраних заходів та гарантій.

2.1.3 Елементи, які слід взяти до уваги

17. Стаття 25(1) перераховує елементи, які контролер повинен враховувати при визначенні заходів для конкретної операції з обробки. Далі ми надамо рекомендації щодо застосування цих елементів у процесі розроблення, який включає розроблення стандартних налаштувань. Усі ці елементи сприяють визначенню того, чи підходить той чи інший захід для ефективного впровадження принципів. Таким чином, кожен із цих елементів не є самоціллю, а є факторами, які слід розглядати разом для досягнення мети.

2.1.3.1 «сучасний рівень розвитку»

18. Поняття «сучасніший рівень розвитку» присутнє в різних нормативно-правових актах ЄС, наприклад, у сфері захисту довкілля та безпеки продукції. У GDPR посилання на «сучасніший

[6] «Основоположні принципи, що застосовуються до контролерів (тобто законність, мінімізація даних, обмеження цілей, прозорість, цілісність даних, точність даних) повинні залишатися незмінними, незалежно від обробки та ризиків для суб'єктів даних. Однак належна увага до специфіки та обсягу такої обробки завжди була невід'ємною частиною застосування цих принципів, тому вони за своєю суттю є масштабованими». Робоча група за статтею 29. «Заява про роль підходу, заснованого на оцінці ризиків, у правовій базі захисту даних». РД 218, 30 травня 2014 року, с. 3. ec.europa.eu/iustice/article-29/documentation/opinion-recommendation/files/2014/wp218 en.pdf

[7] Див. преамбули 74 і 78.

рівень розвитку»[8] міститься не лише в статті 32, де йдеться про заходи безпеки, [910]а й у статті 25, що поширює цей критерій на всі технічні та організаційні заходи, які застосовуються в процесі обробки.

19. У контексті статті 25 посилання на «сучасний рівень розвитку» накладає на контролерів зобов'язання при визначенні відповідних технічних та організаційних заходів **брати до уваги поточний прогрес у технологіях**, доступних на ринку. Вимога полягає в тому, що контролери мають бути обізнані та бути в курсі технологічного прогресу; як технологія може створювати ризики або можливості для захисту даних у процесі обробки; як впроваджувати та оновлювати заходи та гарантії, що *забезпечують ефективну реалізацію* принципів та прав суб'єктів даних, беручи до уваги технологічний ландшафт, що розвивається.

20. «Сучасний рівень розвитку» — це динамічна концепція, яка не може бути статично визначена у фіксований момент часу, а повинна *постійно* оцінюватися в контексті технологічного прогресу. В умовах технологічного прогресу контролер може виявити, що захід, який колись забезпечував належний рівень захисту, більше не забезпечує його. Таким чином, нехтування технологічними змінами може призвести до недотримання вимог статті 25.

21. Критерій «сучасного рівня розвитку» стосується не лише технологічних, але й організаційних заходів. Відсутність відповідних організаційних заходів може знизити або навіть повністю підірвати ефективність обраної технології. Прикладами організаційних заходів можуть бути прийняття внутрішньої політики; сучасне навчання з питань технологій, безпеки та захисту даних; а також політика управління та менеджменту IT-безпеки.

22. Існуючі та визнані рамки, стандарти, сертифікації, кодекси поведінки тощо в різних галузях можуть відігравати певну роль у визначенні «сучасного рівня розвитку» у певній сфері використання. Якщо такі стандарти існують і забезпечують високий рівень захисту суб'єкта даних відповідно до вимог законодавства або виходять за його межі, контролери повинні брати їх до уваги при розробленні та впровадженні заходів із захисту даних.

2.1.3.2 «витрати на реалізацію»

23. Контролер може враховувати витрати на реалізацію при виборі та застосуванні відповідних технічних та організаційних заходів та необхідних гарантій, які ефективно впроваджують принципи з метою захисту прав суб'єктів даних. Витрати стосуються ресурсів у цілому, включаючи час і людські ресурси.

---

[8] Рішення Федерального конституційного суду Німеччини у справі «Калькар» 1978 року: https://germanlawarchive.iuscomp.org/?p=67 може стати основою для методології об'єктивного визначення цього поняття. Виходячи із цього, «сучасний рівень розвитку» технологій буде визначатися між «існуючими науковими знаннями та дослідженнями» та більш усталеними «загальноприйнятими правилами технологій». Таким чином, «сучасний рівень розвитку» можна визначити як технологічний рівень послуги, технології або продукту, який існує на ринку і є найефективнішим для досягнення поставлених цілей.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

Прийнято

24. Елемент витрат не вимагає від контролера витрачати непропорційно велику кількість ресурсів, якщо існують альтернативні, менш ресурсоємні, але ефективні заходи. Однак витрати на реалізацію є фактором, який слід враховувати для впровадження захисту даних за призначенням, а не підставою для відмови від його впровадження.

25. Таким чином, обрані заходи повинні гарантувати, що діяльність з обробки, передбачена контролером, не обробляє персональні дані з порушенням принципів, незалежно від витрат. Контролери повинні мати можливість управляти загальними витратами, щоб мати змогу ефективно впроваджувати всі принципи та, відповідно, захищати права.

2.1.3.3 «специфіка, обсяг, контекст і цілі обробки»

26. Контролери повинні враховувати специфіку, обсяг, контекст і цілі обробки при визначенні необхідних заходів.

27. Ці фактори слід тлумачити відповідно до їхньої ролі в інших положеннях GDPR, таких як статті 24, 32 і 35, з метою впровадження принципів захисту даних у процесі обробки.

28. Коротко кажучи, поняття **специфіки** можна розуміти як невід'ємні[11] характеристики обробки. **Обсяг** стосується масштабу та діапазону обробки. **Контекст** стосується обставин обробки, які можуть вплинути на очікування суб'єкта даних, тоді як **цілі** стосуються цілей обробки.

2.1.3.4 «ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які може спричинити обробку даних»

29. GDPR застосовує послідовний підхід, заснований на оцінці ризиків, у багатьох своїх положеннях, зокрема у статтях 24, 25, 32 та 35, з метою визначення відповідних технічних та організаційних заходів для захисту фізичних осіб, їхніх персональних даних та дотримання вимог GDPR. Об'єкти захисту завжди однакові (фізичні особи через захист їхніх персональних даних), від однакових ризиків (для прав фізичних осіб), з урахуванням однакових умов (специфіки, обсягу, контексту та цілей обробки).

30. Здійснюючи аналіз ризиків на відповідність статті 25, контролер повинен виявити ризики для прав суб'єктів даних, які створює порушення принципів, а також визначити їх ймовірність та тяжкість, щоб вжити заходів для ефективного зменшення виявлених ризиків. Систематична та ретельна оцінка обробки має вирішальне значення при проведенні оцінки ризиків. Наприклад, контролер оцінює конкретні ризики, пов'язані з відсутністю вільно наданої згоди, що є порушенням принципу законності, під час обробки персональних даних дітей та молодих людей віком до 18 років як вразливої групи, у випадку, коли не існує інших законних підстав, та вживає відповідних заходів для усунення й ефективного зменшення виявлених ризиків, пов'язаних із цією групою суб'єктів даних.

---

[11] Прикладами є спеціальні категорії персональних даних, автоматичне прийняття рішень, викривлені владні відносини, непередбачувана обробка, труднощі для суб'єкта даних у здійсненні прав тощо.

31. «Настанови EDPB щодо оцінки впливу на захист даних (DPIA)»[12], які зосереджені на визначенні того, чи може операція з обробки даних призвести до високого ризику для суб'єкта даних, також надають вказівки щодо того, як оцінювати ризики для захисту даних та як проводити оцінку ризиків для захисту даних. Ці Настанови також можуть бути корисними під час оцінки ризиків у всіх статтях, згаданих вище, включаючи статтю 25.

32. Підхід, заснований на оцінці ризиків, не виключає використання базових показників, найкращих практик і стандартів. Вони можуть стати корисним інструментарієм для контролерів для подолання подібних ризиків у схожих ситуаціях (специфіка, обсяг, контекст і цілі обробки). Однак зобов'язання статті 25 (а також статей 24, 32 і 35(7)(c)) враховувати *«ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які може спричинити обробка даних»* залишається чинним. Тому контролери, попри підтримку таких інструментів, завжди повинні проводити оцінку ризиків для захисту даних у кожному конкретному випадку для відповідної діяльності з обробки та перевіряти ефективність запропонованих заходів і гарантій. У такому випадку може виникнути потреба у проведенні оцінки впливу на захист даних або оновленні існуючої оцінки впливу на захист даних.

2.1.4 Часовий аспект

2.1.4.1 На момент визначення засобів для обробки

33. Захист даних за призначенням має реалізуватися «*під час визначення засобів для обробки*».

34. *«Засоби обробки»* охоплюють як загальні, так і детальні елементи розроблення процесу обробки, включаючи архітектуру, процедури, протоколи, макет та зовнішній вигляд.

35. *«Час визначення засобів для обробки»* означає період часу, коли контролер вирішує, як буде проводитися обробка, а також спосіб, у який буде відбуватися обробка, і механізми, які будуть використовуватися для проведення такої обробки. Саме в процесі прийняття таких рішень контролер повинен оцінити відповідні заходи та гарантії для ефективної імплементації принципів і прав суб'єктів даних у процесі обробки, а також врахувати такі елементи, як сучасний рівень розвитку, витрати на реалізацію, специфіку, обсяг, контекст та цілі, а також ризики. Сюди входить час на закупівлю та впровадження програмного забезпечення, обладнання та послуг для обробки даних.

36. Завчасний розгляд принципів захисту даних за призначенням і за замовчуванням має вирішальне значення для успішної реалізації принципів та захисту прав суб'єктів даних. Крім того, з точки зору витрат та вигод, контролери також зацікавлені в тому, щоб врахувати принципи захисту даних за призначенням і за замовчуванням раніше, ніж пізніше, оскільки подальше внесення змін до вже розроблених планів та операцій з обробки даних може бути складним та дорогим завданням.

---

[12] Робоча група за статтею 29 «Настанови щодо оцінки впливу на захист даних (DPIA) та визначення того, чи обробка «може призвести до високого ризику» для цілей Регламенту 2016/679». РД 248, версія 01, 4 жовтня 2017 року. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – схвалений EDPB.
Прийнято

2.1.4.2 Під час самої обробки (підтримка та перегляд вимог щодо захисту даних)

37. Після початку обробки контролер має постійний обов'язок підтримувати принципи захисту даних за призначенням і за замовчуванням, тобто продовжувати ефективну реалізацію принципів з метою захисту прав, бути в курсі сучасного рівня розвитку, переоцінювати рівень ризику тощо. Специфіка, обсяг і контекст операцій з обробки, а також ризик можуть змінюватися в процесі обробки, а це означає, що контролер повинен переоцінювати свої операції з обробки за допомогою регулярних перевірок та оцінок ефективності обраних ним заходів і гарантій.

38. Зобов'язання з підтримки, перегляду та оновлення, за необхідності, операцій з обробки також поширюється на вже існуючі системи. Це означає, що застарілі системи, розроблені до набрання чинності GDPR, повинні проходити перевірку та обслуговування, щоб забезпечити реалізацію заходів і гарантій, які ефективно реалізують принципи та права суб'єктів даних, як зазначено в цих Настановах.

39. Це зобов'язання також поширюється на будь-яку обробку, що здійснюється за допомогою операторів даних. Операції операторів повинні регулярно перевірятися та оцінюватися контролерами, щоб гарантувати, що вони забезпечують постійне дотримання принципів і дозволяють контролеру даних виконувати свої відповідні зобов'язання.

2.2 Стаття 25(2): Захист даних за замовчуванням

2.2.1 За замовчуванням обробляються лише ті персональні дані, які необхідні для кожної конкретної мети обробки

40. «За замовчуванням», згідно із загальним визначенням у комп'ютерних науках, означає попередньо встановлене або попередньо вибране значення сконфігурованого параметра, яке присвоюється програмному забезпеченню, комп'ютерній програмі або пристрою. Такі налаштування також називають «пресетами» або «заводськими налаштуваннями», особливо для електронних пристроїв.

41. Таким чином, термін «за замовчуванням» при обробці персональних даних означає вибір значень конфігурації або параметрів обробки, які встановлені або прописані в системі обробки, наприклад, у програмному додатку, службі або пристрої, або в ручній процедурі обробки, які впливають на обсяг зібраних персональних даних, ступінь їх обробки, період їх зберігання і доступність.

42. Контролер повинен обирати й несе відповідальність за реалізацію налаштувань та опцій обробки за замовчуванням таким чином, щоб за замовчуванням здійснювалося лише та обробка, яка є суворо необхідною для досягнення встановленої законної мети. Тут контролери повинні покладатися на свою оцінку необхідності обробки з точки зору правових підстав, передбачених статтею 6(1). Це означає, що за замовчуванням контролер не повинен збирати більше даних, ніж це необхідно, не повинен обробляти зібрані дані більше, ніж це необхідно для його цілей, і не повинен зберігати дані довше, ніж це необхідно. Основна вимога полягає в тому, щоб захист даних був вбудований у процес обробки за замовчуванням.

43. Контролер зобов'язаний заздалегідь визначити, для яких конкретних, чітких і законних цілей збираються та обробляються персональні дані. [13] Заходи за замовчуванням мають бути відповідними, щоб забезпечити обробку лише тих персональних даних, які необхідні для кожної конкретної мети обробки. «Керівництво з оцінки необхідності та пропорційності заходів, що обмежують право на захист персональних даних» EDPS може бути корисним також для вирішення питання про те, які дані необхідно обробляти для досягнення конкретної мети.[14] [15] [16]

44. Якщо контролер використовує програмне забезпечення третьої сторони або готове програмне забезпечення, він повинен провести оцінку ризиків продукту та переконатися, що функції, які не мають законної підстави або не сумісні із передбачуваними цілями обробки, вимкнені.

45. Ті ж самі міркування застосовуються до організаційних заходів, що підтримують операції з обробки. Вони мають бути розроблені таким чином, щоб із самого початку обробляти лише мінімальний обсяг персональних даних, необхідний для конкретних операцій. Це слід особливо враховувати при розподілі доступу до даних між співробітниками, які виконують різні ролі та мають різні потреби в доступі.

46. Таким чином, відповідні «технічні та організаційні заходи» в контексті захисту даних за замовчуванням розуміються так само як обговорювалося вище в підпункті 2.1.1, але застосовуються спеціально для реалізації принципу мінімізації даних.

47. Вищезгадане зобов'язання обробляти лише ті персональні дані, які необхідні для кожної конкретної мети, застосовується до наступних елементів.

2.2.2 Обсяги зобов'язання щодо мінімізації даних

48. Стаття 25(2) перераховує обсяги зобов'язання щодо мінімізації даних для обробки за замовчуванням, зазначаючи, що це зобов'язання поширюється на обсяг зібраних персональних даних, обсяг їхньої обробки, період їхнього зберігання та доступність.

2.2.2.1 «обсяг зібраних персональних даних»

49. Контролери повинні враховувати як обсяг персональних даних, так і типи, категорії та рівень деталізації персональних даних, необхідний для цілей обробки. Їхній вибір повинен враховувати підвищені ризики для принципів цілісності та конфіденційності, мінімізації даних та обмеження

---

[13] Стаття 5(1)(b), (c), (d), (e) GDPR.

[14] Європейський інспектор із захисту даних (EDPS). «Настанови щодо оцінки необхідності та пропорційності заходів, що обмежують право на захист даних». 25 лютого 2019 року. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[15] Див. також EDPS. «Оцінка необхідності заходів, що обмежують основоположне право на захист персональних даних: Інструментарій» https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

[16] Для отримання додаткової інформації про необхідність див. Робочу групу за статтею 29. «Висновок 06/2014 щодо поняття законних інтересів контролера даних відповідно до статті 7 Директиви 95/46/ЄС». РД 217, 9 квітня 2014 року. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
Прийнято

терміну зберігання при зборі великих обсягів детальних персональних даних та порівнювати їх зі зменшенням ризиків при зборі менших обсягів та/або менш детальної інформації про суб'єктів даних. У будь-якому випадку, налаштування за замовчуванням не повинні включати збір персональних даних, які не є необхідними для конкретної мети обробки. Іншими словами, якщо певні категорії персональних даних не є необхідними або якщо детальні дані не потрібні, оскільки достатньо менш деталізованих даних, то будь-які надлишкові персональні дані не повинні збиратися.

50. Ті ж самі вимоги за замовчуванням застосовуються до послуг незалежно від того, яка платформа або пристрій використовується, можуть збиратися лише необхідні для даної мети персональні дані.

2.2.2.2 «ступінь їхньої обробки»

51. Операції з обробки[17] персональних даних обмежуються тим, що є необхідним. Багато операцій з обробки можуть сприяти досягненню цілей обробки. Однак той факт, що певні персональні дані є необхідними для досягнення цілей, не означає, що всі види та частота операцій з обробки можуть здійснюватися над цими даними. Контролери також повинні бути обережними, щоб не виходити за межі «сумісних цілей» статті 6(4), і пам'ятати про те, якою буде обробка в межах обґрунтованих очікувань суб'єктів даних.

2.2.2.3 «термін їх зберігання»

52. Зібрані персональні дані не повинні зберігатися, якщо це не є необхідним для цілей обробки й немає іншої сумісної цілі та законних підстав відповідно до статті 6(4). Будь-яке зберігання має бути об'єктивно обґрунтованим, якщо це необхідно для контролера даних відповідно до принципу підзвітності.

53. Контролер повинен обмежити період зберігання до того, що є необхідним для досягнення цілей. Якщо персональні дані більше не є необхідними для цілей обробки, вони за замовчуванням мають бути видалені або знеособлені. Таким чином, тривалість періоду зберігання буде залежати від цілей обробки, про які йдеться. Це зобов'язання безпосередньо пов'язане з принципом обмеження терміну зберігання в статті 5(1)(e) і має виконуватися за замовчуванням, тобто контролер повинен забезпечити систематичні процедури видалення або знеособлення даних, вбудовані в процес обробки.

---

[17] Відповідно до статті 4(2) GDPR, це включає збір, запис, організацію, структурування, зберігання, адаптацію або зміну, пошук, консультації, використання, розкриття шляхом передачі, розповсюдження або іншого надання, узгодження або комбінування, обмеження, видалення або знищення.

54. Знеособлення[18] персональних даних є альтернативою видаленню за умови, що всі відповідні контекстуальні елементи беруться до уваги, а ймовірність та серйозність ризику, включаючи ризик повторної ідентифікації, регулярно оцінюються.[19]

2.2.2.4 «їхня доступність»

55. Контролер повинен обмежити, хто має доступ і які види доступу до персональних даних на основі оцінки необхідності, а також переконатися, що персональні дані дійсно доступні тим, кому вони потрібні, коли це необхідно, наприклад, у критичних ситуаціях. Контроль доступу повинен застосовуватися до всього потоку даних під час обробки.

56. Стаття 25(2) також зазначає, що персональні дані не повинні бути доступними без втручання фізичної особи невизначеному колу фізичних осіб. Контролер повинен за замовчуванням обмежити доступ і надати суб'єкту даних можливість втрутитися перед публікацією або іншим чином зробити персональні дані про суб'єкта даних доступними невизначеному колу фізичних осіб.

57. Надання персональних даних невизначеному колу осіб може призвести до ще більшого поширення даних, ніж планувалося спочатку. Це особливо актуально в контексті Інтернету та пошукових систем. Це означає, що контролери повинні за замовчуванням надавати суб'єктам даних можливість втручатися до того, як персональні дані стануть у відкритому доступі в Інтернеті. Це особливо важливо, коли йдеться про дітей та вразливі групи.

58. Залежно від правових підстав для обробки, можливість втручання може варіюватися залежно від контексту обробки. Наприклад, запитувати згоду на публічний доступ до персональних даних або мати налаштування конфіденційності, щоб суб'єкти даних могли самі контролювати відкритий доступ.

59. Навіть у випадку, коли персональні дані стають загальнодоступними з дозволу та розуміння суб'єкта даних, це не означає, що будь-який інший контролер, який має доступ до персональних даних, може вільно обробляти їх самостійно для власних цілей — він повинен мати власну законну підставу.[20]

---

[18] Робоча група за статтею 29. «Висновок 05/2014 щодо методів знеособлення». РД 216, 10 квітня 2014 року. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[19] Див. статтю 4(1) GDPR, преамбулу 26 GDPR, Робочу групу за статтею 29 «Висновок 05/2014 щодо методів знеособлення». Також див. підрозділ про «обмеження терміну зберігання» в розділі 3 цього документа, де йдеться про необхідність для контролера забезпечити ефективність впроваджених методів знеособлення.

[20] Див. справу «Satakunnan Markkinapörssi Oy та Satamedia Oy проти Фінляндії», № 931/13.

3 ВПРОВАДЖЕННЯ ПРИНЦИПІВ ЗАХИСТУ ДАНИХ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ, ВИКОРИСТОВУЮЧИ ЗАХИСТ ДАНИХ ЗА ПРИЗНАЧЕННЯМ І ЗА ЗАМОВЧУВАННЯМ

60. На всіх етапах підготовки діяльності з обробки, включаючи закупівлі, тендери, аутсорсинг, розроблення, підтримку, обслуговування, тестування, зберігання, видалення тощо, контролер повинен брати до уваги та враховувати різні елементи захисту даних за призначенням і за замовчуванням, які будуть проілюстровані на прикладах у цій главі в контексті реалізації принципів.[21] [22] [23]

61. Контролери повинні впроваджувати принципи для досягнення захисту даних за призначенням і за замовчуванням. Ці принципи включають: прозорість, законність, справедливість, обмеження цілей, мінімізацію даних, точність, обмеження терміну зберігання, цілісність, конфіденційність та підзвітність. Ці принципи викладені у статті 5 та преамбулі 39 GDPR. Щоб мати повне уявлення про те, як впроваджувати принципи захисту даних за призначенням і за замовчуванням, підкреслюється важливість розуміння значення кожного із цих принципів.

62. Наводячи приклади застосування принципів захисту даних за призначенням і за замовчуванням, ми склали списки **ключових елементів захисту даних за призначенням і за замовчуванням** для кожного із цих принципів. Приклади, висвітлюючи конкретний принцип захисту даних, про який ідеться, можуть перетинатися з іншими тісно пов'язаними принципами. EDPB підкреслює, що ключові елементи та приклади, представлені в цьому документі, не є ні вичерпними, ні обов'язковими, а призначені як керівні елементи для кожного із принципів. Контролери повинні оцінити, як гарантувати дотримання принципів у контексті конкретної операції з обробки, про яку йдеться.

63. Хоча цей розділ зосереджений на впровадженні принципів, контролер також повинен впроваджувати *відповідні* та *ефективні* засоби захисту прав суб'єктів даних, також відповідно до глави III GDPR, якщо це не передбачено самими принципами.

64. Принцип підзвітності є всеосяжним: він вимагає, щоб контролер був відповідальним за вибір необхідних технічних та організаційних заходів.

---

[21] Більше прикладів можна знайти на сайті Норвезького органу захисту даних. «Розроблення програмного забезпечення із захистом даних за призначенням і за замовчуванням». 28 листопада 2017 року. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

Прийнято

3.1 Прозорість[24]

65. Контролер повинен чітко та відкрито інформувати суб'єкта даних про те, як він збиратиме, використовуватиме та передаватиме персональні дані. Прозорість означає надання суб'єктам даних можливості зрозуміти та, за необхідності, скористатися своїми правами, передбаченими статтями 15-22. Цей принцип закріплений у статтях 12, 13, 14 і 34. Заходи та гарантії, запроваджені на підтримку принципу прозорості, повинні також сприяти виконанню цих статей.

66. Ключові елементи за призначенням і за замовчуванням щодо принципу прозорості можуть включати таке:

- Ясність — інформація повинна бути викладена чіткою, стислою та зрозумілою мовою.
- Семантика — повідомлення повинно мати чітке значення для відповідної аудиторії.
- Доступність — інформація повинна бути легко доступною для суб'єкта даних.
- Контекстуальність — інформація повинна надаватися у відповідний час та у відповідній формі.
- Релевантність — інформація повинна бути релевантною та застосовною до конкретного суб'єкта даних.
- Універсальний дизайн — інформація повинна бути доступною для всіх суб'єктів даних, включаючи використання машинозчитуваних мов для полегшення та автоматизації читабельності та ясності.
- Зрозумілість — суб'єкти даних повинні мати чітке розуміння того, чого вони можуть очікувати у зв'язку з обробкою їхніх персональних даних, особливо коли суб'єктами даних є діти або інші вразливі групи.
- Багатоканальність — інформацію слід надавати різними каналами та носіями, а не лише текстовими, щоб підвищити ймовірність того, що інформація ефективно дійде до суб'єкта даних.
- Багаторівневість — інформація повинна бути багаторівневою, щоб вирішити протиріччя між повнотою та розумінням, враховуючи при цьому розумні очікування суб'єктів даних.

Приклад[25]

[24] Детальніше про те, як розуміти поняття «прозорості», можна прочитати в «Робочій групі за статтею 29». «Настанови щодо прозорості відповідно до Регламенту 2016/679». РД 260, версія 01, 11 квітня 2018 року. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – схвалений EDPB

[25] Французький орган захисту даних опублікував кілька прикладів, що ілюструють найкращі практики інформування користувачів, а також інші принципи прозорості: https://design.cnil.fr/en/.

Прийнято

Контролер розробляє політику конфіденційності на своєму вебсайті, щоб відповідати вимогам прозорості. Політика конфіденційності не повинна містити великого обсягу інформації, яку пересічному суб'єкту даних важко зрозуміти та засвоїти. Вона повинна бути написана чіткою та лаконічною мовою, щоб користувач вебсайту міг легко зрозуміти, як обробляються його персональні дані. Тому контролер надає інформацію багаторівнево, виділяючи найважливіші моменти. Більш детальна інформація є у відкритому доступі. Випадаючі меню та посилання на інші сторінки надаються для подальшого пояснення різних пунктів та понять, що використовуються в цій політиці. Контролер також стежить за тим, щоб інформація надавалася в багатоканальному режимі, доповнюючи її відеокліпами для пояснення найважливіших аспектів текстових матеріалів. Синергія між різними сторінками є життєво важливою для того, щоб багаторівневий підхід не посилював плутанину, а навпаки, зменшував її.

Доступ до політики конфіденційності не повинен бути складним для суб'єктів даних. Таким чином, політика конфіденційності є доступною та помітною на всіх вебсторінках відповідного сайту, тож суб'єкт даних завжди може отримати до неї доступ усього в один клік. Надана інформація також розроблена відповідно до найкращих практик та стандартів універсального дизайну, щоб зробити її доступною для всіх.

Крім того, необхідна інформація повинна надаватися в правильному контексті та у відповідний час. Оскільки контролер здійснює багато операцій з обробки даних, використовуючи дані, зібрані на вебсайті, лише загальної політики конфіденційності на вебсайті недостатньо для того, щоб контролер відповідав вимогам прозорості. Тому контролер розробляє інформаційний потік, надаючи суб'єкту даних відповідну інформацію у відповідному контексті, використовуючи, наприклад, інформаційні фрагменти або спливаючі вікна. Наприклад, коли контролер просить суб'єкта даних ввести персональні дані, він інформує суб'єкта даних про те, яким чином ці дані будуть оброблятися та чому ці персональні дані необхідні для обробки.

3.2 Законність

67. Контролер повинен визначити дійсну законну підставу для обробки персональних даних. Заходи та гарантії повинні підтримувати вимогу щодо забезпечення відповідності всього життєвого циклу обробки відповідним правовим підставам для обробки.

68. Ключові елементи за призначенням і за замовчуванням щодо принципу законності можуть включати таке:

- Релеватність — до обробки повинна застосовуватися належна законна підстава.
- Диференціація[26] — законна підстава, що використовується для кожної дії з обробки, повинна бути диференційованою.

[26] EDPB. «Настанови 2/2019 щодо обробки персональних даних відповідно до статті 6(1)(b) GDPR у контексті надання онлайн-послуг суб'єктам даних». Версія 2.0, 8 жовтня 2019 року. Прийнято

- Конкретна мета — відповідна законна підстава повинна бути чітко пов'язана з конкретною метою обробки.[27]
- Необхідність — обробка має бути необхідною та безумовною для того, щоб мета була законною.
- Автономія — суб'єкту даних повинен бути наданий максимально можливий ступінь автономії щодо контролю над персональними даними в рамках законної підстави.
- Отримання згоди — згода повинна надаватися вільно, бути явною, інформованою та однозначною.[28] Особливу увагу слід приділяти здатності дітей та молоді надавати інформовану згоду.
- Відкликання згоди — якщо згода має законну підставу, обробка має сприяти відкликанню згоди. Відкликання має бути таким же простим, як і надання згоди. Якщо це не так, то механізм надання згоди контролера не відповідатиме GDPR.[29]
- Балансування інтересів — якщо законні інтереси мають законну підставу, контролер повинен здійснювати зважене балансування інтересів, приділяючи особливу увагу дисбалансу влади, зокрема, дітям віком до 18 років та іншим вразливим групам. Повинні бути передбачені заходи та гарантії для пом'якшення негативного впливу на суб'єктів даних.
- Визначеність — законна підстава повинна бути встановлена до початку обробки.
- Припинення — якщо законна підстава перестає застосовуватися, обробка має відповідно припинитися.
- Коригування — у разі дійсної зміни законної підстави для обробки даних, фактична обробка має бути скоригована відповідно до нової законної підстави.[30]
- Розподіл відповідальності — якщо передбачається спільний контроль, сторони повинні чітко та прозоро розподілити свої обов'язки щодо суб'єкта даних і розробити заходи з обробки відповідно до цього розподілу.

Приклад

edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[27] Див. розділ про обмеження цілей нижче.

[28] Настанови 05/2020 щодо надання згоди відповідно до Регламенту 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Настанови 05/2020 щодо надання згоди відповідно до Регламенту 2016/679, с. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] Якщо первинною законною підставою є надання згоди, див. Настанови 05/2020 щодо надання згоди відповідно до Регламенту 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Прийнято

Банк планує запропонувати послугу для підвищення ефективності управління заявками на отримання кредиту. Ідея послуги полягає в тому, що банк, запросивши дозвіл у клієнта, може отримати дані про нього безпосередньо від державних податкових органів. У цьому прикладі не розглядається обробка персональних даних з інших джерел.

Отримання персональних даних про фінансовий стан суб'єкта персональних даних необхідне для того, щоб вжити заходів на вимогу суб'єкта персональних даних до укладення кредитного договору.[31] Однак збір персональних даних безпосередньо від податкової служби не вважається необхідним, оскільки клієнт може укласти договір, надавши інформацію з податкової служби самостійно. Хоча банк може мати законний інтерес в отриманні документації безпосередньо від податкових органів, наприклад, для забезпечення ефективності процесу оформлення кредиту, надання банкам такого прямого доступу до персональних даних заявників створює ризики, пов'язані з використанням або потенційним зловживанням правами доступу.

Реалізуючи принцип законності, контролер усвідомлює, що в цьому контексті він не може використовувати підставу «необхідності для виконання договору» для тієї частини обробки, яка передбачає збір персональних даних безпосередньо від податкових органів. Той факт, що це конкретна обробка становить ризик того, що суб'єкт даних стане менш залученим до обробки своїх даних, також є важливим фактором в оцінці законності самої обробки. Банк доходить висновку, що ця частина обробки повинна спиратися на іншу законну підставу обробки. У конкретній державі-члені, де знаходиться контролер, існує національне законодавство, яке дозволяє банку збирати інформацію безпосередньо від державних податкових органів, якщо суб'єкт даних дав на це попередню згоду.

Тому банк представляє інформацію про обробку на платформі онлайн-заявки таким чином, щоб суб'єктам даних було легко зрозуміти, яка обробка є обов'язковою, а яка — необов'язковою. Варіанти обробки за замовчуванням не дозволяють отримувати дані безпосередньо з інших джерел, окрім самого суб'єкта даних, а варіант прямого отримання інформації представлений таким чином, щоб не утримувати суб'єкта даних від відмови. Будь-яка згода, надана на збір даних безпосередньо від інших контролерів, є тимчасовим правом доступу до певного набору інформації.

Будь-яка надана згода обробляється в електронному вигляді та документується, а суб'єктам даних надається простий спосіб контролювати те, на що вони погодилися, та відкликати свою згоду.

Контролер заздалегідь оцінив ці вимоги захисту даних за призначенням і за замовчуванням та включив усі ці критерії у свою специфікацію вимог до тендеру на закупівлю платформи. Контролер усвідомлює, що якщо він не включить вимоги із захисту даних за призначенням і за замовчуванням до тендеру, впровадження захисту даних згодом може бути або занадто пізнім, або дуже дорогим процесом.

[31] Див. статтю 6(1)(b) GDPR.

3.3 Справедливість

69. Справедливість — це всеохоплюючий принцип, який вимагає, щоб персональні дані не оброблялися у спосіб, який є невиправдано шкідливим, незаконно дискримінаційним, несподіваним або таким, що вводить в оману суб'єкта даних. Заходи та гарантії, що реалізують принцип справедливості, також підтримують права й свободи суб'єктів даних, зокрема право на інформацію (прозорість), право на втручання (доступ, видалення, перенесення даних, виправлення) та право на обмеження обробки (право не бути об'єктом автоматизованого прийняття індивідуальних рішень та заборона дискримінації суб'єктів даних у таких процесах).

70. Ключові елементи за призначенням і за замовчуванням щодо принципу справедливості можуть включати таке:

- Автономія — суб'єктам даних повинен бути наданий максимально можливий ступінь автономії у визначенні способу використання їхніх персональних даних, а також обсягу та умов такого використання або обробки.
- Взаємодія — суб'єкти даних повинні мати можливість спілкуватися та реалізовувати свої права щодо персональних даних, які обробляються контролером.
- Очікування — обробка має відповідати обґрунтованим очікуванням суб'єктів даних.
- Заборона дискримінації — контролер не повинен несправедливо дискримінувати суб'єктів даних.
- Заборона експлуатації — контролер не повинен експлуатувати потреби чи вразливості суб'єктів даних.
- Вибір споживача — контролер не повинен «прив'язувати» своїх користувачів у несправедливий спосіб. Якщо сервіс, що обробляє персональні дані, є приватною власністю, він може створювати прив'язку до сервісу, що може бути несправедливим, якщо це обмежує можливість суб'єктів даних реалізовувати своє право на перенесення даних відповідно до статті 20.
- Баланс повноважень — баланс повноважень має бути ключовою метою відносин між контролером та суб'єктом даних. Слід уникати дисбалансу влади. Якщо це неможливо, вони повинні бути визнані та враховані за допомогою відповідних контрзаходів.
- Відсутність передачі ризиків — контролери не повинні передавати ризики підприємства суб'єктам даних.
- Відсутність обману — інформація про обробку даних і доступні варіанти має надаватися об'єктивно та нейтрально, без використання оманливої або маніпулятивної мови чи оформлення.
- Поважання прав — контролер повинен поважати основоположні права суб'єктів даних та вживати відповідних заходів і гарантій, а також не порушувати ці права, якщо тільки це прямо не передбачено законом.
- Етичність — контролер повинен враховувати ширший вплив обробки даних на права та гідність людей.
- Правдивість — контролер повинен надавати інформацію про те, як він обробляє персональні дані, діяти так, як він заявляє, і не вводити в оману суб'єктів даних.
- Людське втручання — контролер повинен забезпечити *кваліфіковане* людське втручання, здатне виявляти упередження, які можуть виникати через роботу

обладнання, відповідно до права не підлягати автоматизованому прийняттю індивідуальних рішень, передбаченого статтею 22.[32]

- Справедливі алгоритми — регулярна оцінка того, чи функціонують алгоритми відповідно до цілей, і коригування алгоритмів для пом'якшення виявлених упереджень та забезпечення справедливості в процесі обробки. Суб'єкти даних повинні бути поінформовані про функціонування обробки персональних даних на основі алгоритмів, які аналізують або роблять прогнози щодо них, таких як результати роботи, економічне становище, здоров'я, особисті уподобання, надійність або поведінка, місцезнаходження або пересування. [33]

Приклад 1

Контролер керує пошуковою системою, яка обробляє переважно персональні дані, створені користувачами. Контролеру вигідно мати великі обсяги персональних даних і мати можливість використовувати їх для таргетованої реклами. Тому контролер бажає впливати на суб'єктів даних, щоб дозволити більш широкий збір та використання їхніх персональних даних. Згода має бути отримана шляхом надання суб'єкту даних варіантів обробки.

Реалізуючи принцип справедливості, беручи до уваги специфіку, обсяг, контекст і цілі обробки, контролер усвідомлює, що він не може представити варіанти таким чином, щоб підштовхнути суб'єкта даних до того, щоб дозволити контролеру зібрати більше персональних даних, ніж якби варіанти були представлені в рівній і нейтральній формі. Це означає, що вони не можуть представляти варіанти обробки таким чином, щоб суб'єктам даних було складно утриматися від надання своїх даних або щоб суб'єктам даних було складно змінити свої налаштування конфіденційності та обмежити обробку. Це приклади «темних схем», які суперечать духу статті 25. Варіанти обробки за замовчуванням не повинні бути інвазивними, а вибір подальшої обробки повинен бути представлений таким чином, щоб не чинити тиск на суб'єкта даних, щоб він дав згоду. Тому контролер представляє варіанти надання згоди або утримання як два однаково видимі варіанти, точно відображаючи наслідки кожного з них для суб'єкта даних.

Приклад 2

Інший контролер обробляє персональні дані для надання послуги потокового мовлення, де користувачі можуть вибирати між звичайною підпискою зі стандартною якістю та преміум-підпискою з вищою якістю. У рамках преміум-підписки абоненти отримують пріоритетне обслуговування.

[32] Див. Настанови щодо автоматизованого прийняття індивідуальних рішень та профілювання для цілей Регламенту 2016/679.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826

[33] Див. преамбулу 71 GDPR.

Прийнято

Що стосується принципу справедливості, то пріоритетне обслуговування, що надається преміум-підписникам, не може дискримінувати доступ звичайних підписників до реалізації їхніх прав відповідно до статті 12 GDPR. Це означає, що хоча преміум-абоненти отримують пріоритетне обслуговування, така пріоритетність не може призвести до відсутності належних заходів для реагування на запити звичайних абонентів без невиправданої затримки та в будь-якому випадку протягом одного місяця з моменту отримання запитів.

Пріоритетні клієнти можуть платити за отримання кращого обслуговування, але всі суб'єкти даних повинні мати рівний і недискримінаційний доступ до реалізації своїх прав і свобод, як того вимагає стаття 12.

3.4 Обмеження цілей[34]

71. Контролер повинен збирати дані для визначених, чітких та законних цілей і не обробляти їх у спосіб, несумісний із цілями, для яких вони були зібрані.[35] Таким чином, структура обробки повинна визначатися тим, що необхідно для досягнення цих цілей. Якщо має відбутися будь-яка подальша обробка, контролер повинен спочатку переконатися, що ця обробка має цілі, сумісні з початковими цілями, і розробити таку обробку відповідним чином. Сумісність нової мети повинна оцінюватися відповідно до критеріїв, викладених у статті 6(4).

72. Ключові елементи за призначенням і за замовчуванням щодо принципу обмеження цілей можуть включати таке:

- Визначеність — законні цілі повинні бути визначені до планування обробки.
- Конкретність — цілі повинні бути конкретними та чіткими щодо того, для чого обробляються персональні дані.
- Орієнтація на цілі — цілі обробки мають керувати розробленням обробки та встановлювати межі обробки.
- Необхідність — цілі визначають, які персональні дані необхідні для обробки.
- Сумісність — будь-які нові цілі повинні бути сумісними з первісними цілями, для яких збиралися дані, і визначати відповідні зміни в проектуванні.
- Обмеження подальшої обробки — контролер не повинен об'єднувати набори даних або виконувати будь-яку подальшу обробку для нових несумісних цілей.
- Обмеження повторного використання — контролер повинен використовувати технічні заходи, включаючи хешування та шифрування, щоб обмежити можливість повторного використання персональних даних. Контролер також повинен вживати організаційних

[34] Робоча група за статтею 29 надала вказівки щодо розуміння принципу обмеження цілей відповідно до Директиви 95/46/ЄС. Хоча Висновок не прийнятий EDBP, він все ще може бути актуальним, оскільки формулювання принципу є таким самим у GDPR. Робоча група за статтею 29. «Висновок 03/2013 щодо обмеження цілей». РД 203, 2 квітня 2013 року. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Стаття 5(1)(b) GDPR.

заходів, таких як політика та договірні зобов'язання, які обмежують повторне використання персональних даних.

- Перевірка — контролер повинен регулярно перевіряти, чи є обробка необхідною для цілей, для яких були зібрані дані, і перевіряти проектування на предмет обмеження цілей.

Приклад

Контролер обробляє персональні дані своїх клієнтів. Метою обробки є виконання договору, тобто можливість доставити товар на правильну адресу та отримати оплату. Зберігаються такі персональні дані, як історія покупок, ім'я, адреса, адреса електронної пошти та номер телефону.

Контролер розглядає можливість придбання продукту для системи управління взаємовідносинами з клієнтами (CRM), яка збирає всі дані про клієнтів, їхні продажі, маркетинг та обслуговування в одному місці. Продукт дає можливість зберігати всі телефонні дзвінки, дії, документи, електронні листи та маркетингові кампанії, щоб отримати всестороннє уявлення про клієнта. Крім того, CRM здатна автоматично аналізувати купівельну спроможність клієнтів, використовуючи публічну інформацію. Мета аналізу — краще таргетувати рекламну діяльність. Ця діяльність не є частиною початкової законної цілі обробки.

Щоб відповідати принципу обмеження цілей, контролер вимагає від постачальника продукту зіставити різні види діяльності з обробки, у яких використовуються персональні дані, з цілями, релевантними для контролера.

Після отримання результатів такого зіставлення контролер оцінює, чи сумісні нова маркетингова мета та мета цільової реклами з початковими цілями, визначеними під час збору даних, і чи існує достатня законна підстава для відповідної обробки. Якщо оцінка не дає позитивної відповіді, контролер не повинен продовжувати використовувати відповідні функції. Крім того, контролер може відмовитися від оцінки й просто не використовувати описані функціональні можливості продукту.

3.5 Мінімізація даних

73. Обробці підлягають лише ті персональні дані, які є повними, релевантними та обмежуються лише тим, що **необхідно** для досягнення мети.[36] Як наслідок, контролер повинен заздалегідь визначити, які функції та параметри систем обробки та їхніх допоміжних функцій є допустимими. Мінімізація даних обґрунтовує та реалізує принцип необхідності. Під час подальшої обробки контролер повинен періодично розглядати, чи оброблені персональні дані все ще є повними, релевантними та необхідними, або ж дані мають бути видалені чи знеособлені.

74. Контролери повинні насамперед визначити, чи потрібно взагалі обробляти персональні дані для відповідних цілей. Контролер повинен перевірити, чи можна досягти відповідних цілей,

[36] Стаття 5(1)(c) GDPR.

обробляючи менший обсяг персональних даних, або маючи менш деталізовані чи агреговані персональні дані, або взагалі не обробляючи персональні дані[37]. Така перевірка повинна відбуватися до початку будь-якої обробки, але також може здійснюватися в будь-який момент протягом життєвого циклу обробки. Це також узгоджується зі статтею 11.

75. Мінімізація може також стосуватися ступеня ідентифікації. Якщо цілі обробки не вимагають, щоб кінцевий набір даних стосувався ідентифікованої особи або особи, яку можна ідентифікувати (наприклад, у статистиці), але початкова обробка вимагає цього (наприклад, перед агрегуванням даних), то контролер повинен видалити або знеособити персональні дані, як тільки ідентифікація більше не потрібна. Або, якщо подальша ідентифікація необхідна для інших видів обробки, персональні дані повинні бути псевдонімізовані, щоб зменшити ризики для прав суб'єктів даних.

76. Ключові елементи за призначенням і за замовчуванням щодо принципу мінімізації даних можуть включати таке:

- Уникнення обробки даних — повне уникнення обробки персональних даних, якщо це можливо для відповідної мети.
- Обмеження — обмеження обсягу зібраних персональних даних до того, що є необхідним для досягнення мети.
- Обмеження доступу — організація обробки даних таким чином, щоб мінімальна кількість людей мала доступ до персональних даних для виконання своїх обов'язків, і відповідно обмежений доступ.
- Релевантність — персональні дані повинні бути релевантними для відповідної обробки, і контролер повинен продемонструвати цю релевантність.
- Необхідність — кожна категорія персональних даних повинна бути необхідною для визначених цілей і повинна оброблятися лише в тому випадку, якщо неможливо досягти мети іншими способами.
- Агрегація — використання агрегованих даних, коли це можливо.
- Псевдонімізація — псевдонімізація персональних даних, як тільки відпадає необхідність мати персональні дані, що дозволяють безпосередньо ідентифікувати особу, та зберігання ідентифікаційних ключів окремо.
- Знеособлення та видалення — якщо персональні дані не є необхідними або більше не є необхідними для досягнення мети, персональні дані повинні бути знеособлені або видалені.
- Потік даних — потік даних повинен бути достатньо ефективним, щоб не створювати більше копій, ніж це необхідно.
- «Сучасний рівень розвитку» — контролер повинен застосовувати сучасні та відповідні технології для уникнення та мінімізації даних.

Приклад 1

[37] Про це йдеться у преамбулі 39 GDPR: «...Персональні дані необхідно обробляти, лише якщо мети обробки не можна обґрунтовано досягнути іншими засобами».

Книгарня хоче збільшити свій дохід, продаючи книги онлайн. Власник книгарні хоче створити стандартизовану форму для процесу замовлення. Щоб переконатися, що клієнти заповнюють всю необхідну інформацію, власник книгарні робить усі поля форми обов'язковими для заповнення (якщо ви не заповните всі поля, клієнт не зможе оформити замовлення). Спочатку власник інтернет-магазину використовує стандартну контактну форму, яка запитує інформацію, включаючи дату народження, номер телефону та домашню адресу покупця. Однак не всі поля у формі є необхідними для купівлі та доставки книжок. У цьому конкретному випадку, якщо суб'єкт даних платить за товар наперед, дата народження та номер телефону не є необхідними для придбання товару. Це означає, що ці поля не можуть бути обов'язковими для заповнення у вебформі для замовлення продукту, якщо контролер не зможе чітко обґрунтувати, чому їх заповнення є необхідним. Крім того, існують ситуації, коли адреса не є необхідною. Наприклад, замовляючи електронну книгу, клієнт може завантажити продукт безпосередньо на свій пристрій.

Тому власник інтернет-магазину вирішує створити дві вебформи: одну для замовлення книжок з полем для адреси покупця, а іншу — для замовлення електронних книжок без поля для адреси покупця.

Приклад 2

Підприємство громадського транспорту хоче збирати статистичну інформацію на основі маршрутів пасажирів. Це корисно для прийняття правильних рішень щодо змін у розкладі руху громадського транспорту та правильних маршрутів поїздів. Пасажири повинні прикладати свій квиток до зчитувального пристрою щоразу, коли вони входять або виходять із транспортного засобу. Здійснивши оцінку ризиків, пов'язаних із правами та свободами пасажирів, щодо збору інформації про маршрути пересування пасажирів, контролер встановив, що ідентифікувати пасажирів в умовах, коли вони проживають або працюють у малонаселених районах, можливо на основі одноразової ідентифікації маршруту завдяки ідентифікатору квитка. Тому, оскільки це не є необхідним для оптимізації розкладу руху громадського транспорту та маршрутів поїздів, контролер не зберігає ідентифікатор квитка. Після завершення поїздки контролер зберігає лише окремі маршрути, щоб не мати змоги ідентифікувати поїздки, пов'язані з одним квитком, а лише зберігає інформацію про окремі маршрути.

У випадках, коли все ще існує ризик ідентифікації особи виключно за її маршрутом руху в громадському транспорті, контролер застосовує статистичні заходи для зменшення цього ризику, наприклад, скорочення початку та кінця маршруту.

Прийнято

Приклад 3

Кур'єр має на меті оцінити ефективність своїх доставок з точки зору часу доставки, планування робочого навантаження та споживання палива. Для досягнення цієї мети кур'єру доводиться обробити низку персональних даних, що стосуються як працівників (водіїв), так і клієнтів (адреси, товари, що доставляються тощо). Ця операція з обробки пов'язана з ризиками як моніторингу працівників, що вимагає певних правових гарантій, так і відстеження звичок клієнтів через знання про доставлені товари з плином часу. Ці ризики можна суттєво зменшити за допомогою відповідної псевдонімізації працівників та клієнтів. Зокрема, якщо ключі псевдонімізації часто змінюються, а замість детальних адрес розглядаються макрозони, досягається ефективна мінімізація даних, і контролер може зосередитися виключно на процесі доставки та оптимізації ресурсів, не переступаючи межі моніторингу поведінки окремих осіб (клієнтів або працівників).

Приклад 4

Лікарня збирає дані про своїх пацієнтів у лікарняній інформаційній системі (електронній медичній картці). Персонал лікарні повинен мати доступ до файлів пацієнтів, щоб приймати обґрунтовані рішення щодо догляду та лікування пацієнтів, а також для документування всіх вжитих діагностичних, доглядових та лікувальних заходів. За замовчуванням доступ надається лише тим членам медичного персоналу, які призначені для лікування відповідного пацієнта у профільному відділенні, до якого він прикріплений. Коло осіб, які мають доступ до медичної картки пацієнта, розширюється, якщо до лікування залучаються інші відділення або діагностичні підрозділи. Після виписки пацієнта й завершення виставлення рахунків доступ обмежується до невеликої групи працівників у кожному відділенні, які відповідають на запити про медичну інформацію або консультації, зроблені або запитані іншими постачальниками медичних послуг, з дозволу відповідного пацієнта.

3.6 Точність

77. Персональні дані повинні бути точними й підтримуватися в актуальному стані, і повинні бути вжиті всі необхідні заходи для забезпечення того, щоб персональні дані, які є неточними, з огляду на цілі, для яких вони обробляються, були видалені або виправлені без зволікання.[38]

78. Вимоги слід розглядати у зв'язку з ризиками та наслідками конкретного використання даних. Неточні персональні дані можуть становити ризик для прав і свобод суб'єктів даних, наприклад, коли вони призводять до помилкового діагнозу або неправомірного лікування в рамках медичного протоколу, а неправильне зображення особи може призвести до прийняття рішень на неправильній основі або власноруч, або за допомогою автоматизованого прийняття рішень, або за допомогою штучного інтелекту.

79. Ключові елементи за призначенням і за замовчуванням щодо принципу точності можуть включати таке:

[38] Стаття 5(1)(d) GDPR.

- Джерело даних — джерела персональних даних повинні бути надійними з точки зору точності даних.
- Ступінь точності — кожен елемент персональних даних повинен бути настільки точним, наскільки це необхідно для визначених цілей.
- Оцінювана точність — зменшити кількість хибнопозитивних/хибнонегативних результатів, наприклад, упереджень в автоматизованих рішеннях і штучному інтелекті.
- Верифікація — залежно від характеру даних, а також від того, як часто вони можуть змінюватися, контролер повинен перевіряти правильність персональних даних разом із суб'єктом даних до початку та на різних етапах обробки (наприклад, на предмет відповідності віковим вимогам).
- Видалення/виправлення — контролер повинен негайно видалити або виправити неточні дані. Контролер повинен, зокрема, сприяти цьому, якщо суб'єкти даних є або були дітьми та згодом хочуть видалити такі персональні дані.[39]
- Уникнення розповсюдження помилок — контролери повинні пом'якшити вплив накопичених помилок у ланцюжку обробки.
- Доступ — суб'єкти даних повинні мати інформацію про персональні дані та ефективний доступ до них відповідно до статей 12-15 GDPR з метою контролю точності та виправлення помилок за необхідності.
- Постійна точність — персональні дані повинні бути точними на всіх етапах обробки, перевірки точності повинні проводитися на критичних етапах.
- Актуальність — персональні дані повинні оновлюватися, якщо це необхідно для досягнення мети.
- Проектування даних — використання технологічних та організаційних особливостей проектування для зменшення неточності, наприклад, представлення стислих заздалегідь визначених варіантів відповідей замість вільних текстових полів.

Приклад 1

Страхова компанія хоче використовувати штучний інтелект (ШІ) для профілювання клієнтів, які купують страхування, як основу для прийняття рішень при розрахунку страхового ризику. Визначаючи, як мають бути розроблені рішення зі ШІ, вони визначають засоби обробки даних і повинні враховувати захист даних при виборі програми для ШІ від постачальника та при прийнятті рішення про те, як навчати ШІ.

Визначаючи спосіб навчання ШІ, контролер повинен мати точні дані для досягнення конкретних результатів. Тому контролер повинен переконатися, що дані, які використовуються для навчання ШІ, є точними.

За умови наявності законних підстав для навчання ШІ на основі персональних даних великої підгрупи існуючих клієнтів, контролер обирає групу клієнтів, яка є репрезентативною для населення, щоб уникнути упередженості.

[39] Див. преамбулу 65.

Потім дані про клієнтів збираються з відповідної системи обробки даних, включаючи дані про тип страхування, наприклад, медичне страхування, страхування житла, страхування подорожей тощо, а також дані з державних реєстрів, до яких вони мають законний доступ. Усі дані псевдонімізуються перед передачею в систему, призначену для навчання ШІ-моделі.

Щоб гарантувати, що дані, які використовуються для навчання ШІ, є максимально точними, контролер збирає дані лише з джерел, які містять правильну та актуальну інформацію.

Страхова компанія перевіряє, чи надійний ШІ та чи надає він недискримінаційні результати як під час його розроблення, так і перед випуском продукту на ринок. Коли ШІ повністю навчений і функціонує, страхова компанія використовує результати для оцінки страхових ризиків, але не покладається виключно на ШІ для прийняття рішення про надання страхування, якщо тільки рішення не приймається відповідно до винятків, передбачених статтею 22(2) GDPR.

Страхова компанія також регулярно переглядатиме результати, отримані від ШІ, щоб підтримувати їхню надійність і за необхідності коригувати алгоритм.

Приклад 2

Контролером є медичний заклад, який шукає методи забезпечення цілісності й точності персональних даних у своїх клієнтських реєстрах.

У ситуаціях, коли двоє людей приходять до закладу одночасно й отримують однакове лікування, існує ризик переплутати їх, якщо єдиним параметром, за яким їх можна розрізнити, є ім'я. Для забезпечення точності контролеру потрібен унікальний ідентифікатор для кожної особи, а отже, більше інформації, ніж просто ім'я клієнта.

Установа використовує кілька систем, що містять особисту інформацію клієнтів, і має забезпечити, щоб інформація, пов'язана з клієнтом, була правильною, точною та узгодженою в усіх системах у будь-який момент часу. Установа визначила кілька ризиків, які можуть виникнути, якщо інформація буде змінена в одній системі, але не в інших.

Контролер вирішує зменшити ризик, використовуючи метод хешування, який може бути використаний для забезпечення цілісності даних у журналі лікування. Для записів у журналі лікування та пов'язаних із ними клієнтів створюються незмінні криптографічні позначки часу, щоб будь-які зміни можна було розпізнати, співвіднести та відстежити, якщо це необхідно.

3.7 Обмеження терміну зберігання

80. Контролер повинен забезпечити зберігання персональних даних у формі, яка дозволяє ідентифікувати суб'єктів даних, не довше, ніж це необхідно для цілей, для яких обробляються персональні дані.[40] Дуже важливо, щоб контролер точно знав, які персональні дані компанія

[40] Стаття 5(1)(c) GDPR.

обробляє і чому. Мета обробки повинна бути основним критерієм для прийняття рішення про те, протягом якого терміну зберігати персональні дані.

81. Заходи та гарантії, які реалізують принцип обмеження зберігання, повинні доповнювати права та свободи суб'єктів даних, зокрема, право на видалення та право на заперечення.

82. Ключові елементи за призначенням і за замовчуванням щодо принципу обмеження терміну зберігання можуть включати таке:

- Видалення та знеособлення — контролер повинен мати чіткі внутрішні процедури та функціональні можливості для видалення та/або знеособлення.
- Ефективність знеособлення/видалення — контролер повинен переконатися, що неможливо повторно ідентифікувати знеособлені дані або відновити видалені дані, і повинен перевірити, чи це можливо.
- Автоматизація — видалення певних персональних даних має бути автоматизовано.
- Критерії зберігання — контролер повинен визначити, які дані та тривалість зберігання є необхідними для даної мети.
- Обґрунтування — контролер має обґрунтувати, чому період зберігання необхідний для даної мети та відповідних персональних даних, а також бути в змозі розкрити обґрунтування та правові підстави для терміну зберігання.
- Забезпечення дотримання політики зберігання — контролер повинен забезпечувати дотримання внутрішньої політики зберігання та проводити перевірки того, чи дотримується організація своєї політики на практиці.
- Резервне копіювання/журнали — контролери повинні визначити, які персональні дані й термін зберігання необхідні для резервного копіювання та ведення журналів.
- Потік даних — контролери повинні остерігатися потоку персональних даних та зберігання будь-яких їхніх копій, а також намагатися обмежити їхнє «тимчасове» зберігання.

Приклад

Контролер збирає персональні дані, якщо метою обробки є адміністрування членства суб'єкта даних. Персональні дані видаляються, коли членство припиняється і немає законних підстав для подальшого зберігання даних.

Контролер спочатку розробляє внутрішню процедуру зберігання та видалення даних. Відповідно до неї, працівники повинні власноруч видаляти персональні дані після закінчення терміну зберігання. Працівник дотримується процедури регулярного видалення та виправлення даних з будь-яких пристроїв, резервних копій, журналів, електронної пошти та інших відповідних носіїв інформації.

Щоб зробити видалення більш ефективним і менш схильним до помилок, контролер впроваджує автоматичну систему, яка дозволяє видаляти дані автоматично, надійно і більш регулярно. Система налаштована таким чином, щоб слідувати заданій процедурі видалення даних, яка потім відбувається через заздалегідь визначений регулярний інтервал для видалення персональних даних з усіх носіїв інформації компанії. Контролер регулярно переглядає та тестує процедуру зберігання й забезпечує її відповідність актуальній політиці зберігання.

Прийнято

3.8 Цілісність і конфіденційність

83. Принцип цілісності та конфіденційності включає захист від несанкціонованої або незаконної обробки, а також від випадкової втрати, знищення або пошкодження за допомогою відповідних технічних або організаційних заходів. Безпека персональних даних вимагає відповідних заходів, спрямованих на запобігання інцидентам порушення безпеки даних та управління ними; гарантування належного виконання завдань з обробки даних та дотримання інших принципів; а також сприяння ефективному здійсненню прав фізичних осіб.

84. У преамбулі 78 зазначено, що один із заходів захисту даних за призначенням і за замовчуванням може полягати в наданні контролеру можливості *«створювати та вдосконалювати засоби захисту».* Поряд з іншими заходами захисту даних за призначенням і за замовчуванням, преамбула 78 покладає на контролерів відповідальність за постійну оцінку того, чи використовують вони належні засоби обробки в будь-який час, а також за оцінку того, чи обрані заходи дійсно протидіють існуючим вразливостям. Крім того, контролери повинні проводити регулярні перевірки заходів інформаційної безпеки, які оточують і захищають персональні дані, а також процедури реагування на порушення безпеки даних.

85. Ключові елементи за призначенням і за замовчуванням щодо принципу цілісності та конфіденційності можуть включати таке:

- Система управління інформаційною безпекою (СУІБ) — наявність оперативних засобів управління політиками та процедурами інформаційної безпеки.
- Аналіз ризиків — оцінка ризиків для безпеки персональних даних, враховуючи вплив на права осіб та протидію виявленим ризикам. Для оцінки ризиків необхідно розробити та підтримувати комплексне, систематичне й реалістичне «моделювання загроз» та аналіз поверхні атаки розробленого програмного забезпечення, щоб зменшити вектори атак і можливості використання вразливостей та недоліків у захисті.
- Безпека за призначенням — врахування вимог безпеки на якомога більш ранніх етапах проектування та розроблення системи, а також постійна інтеграція та проведення відповідних тестувань.
- Обслуговування — регулярний перегляд і тестування програмного забезпечення, обладнання, систем і сервісів тощо для виявлення вразливостей систем, що підтримують обробку даних.
- Управління контролем доступу — доступ до персональних даних, необхідних для виконання завдань з обробки, повинен мати лише уповноважений персонал, і контролер повинен розмежовувати привілеї доступу уповноваженого персоналу.
    - Обмеження доступу (уповноважені особи) — організація обробки даних таким чином, щоб мінімальна кількість осіб мала доступ до персональних даних для виконання своїх обов'язків, і відповідно обмеження доступу.
    - Обмеження доступу (зміст) — у контексті кожної операції з обробки обмеження доступу лише до тих атрибутів у наборі даних, які необхідні для виконання цієї операції.
      Крім того, обмеження доступу до даних, що стосуються тих суб'єктів даних, які входять до компетенції відповідного працівника.

Прийнято

- Розмежування доступу — формування обробки даних таким чином, щоб жодна особа не потребувала повного доступу до всіх даних, зібраних про суб'єкта даних, а тим більше до всіх персональних даних певної категорії суб'єктів даних.

- Безпечна передача — передача повинна бути захищена від несанкціонованого та випадкового доступу та змін.
- Безпечне зберігання — зберігання даних має бути захищене від несанкціонованого доступу та змін. Повинні існувати процедури для оцінки ризику централізованого чи децентралізованого зберігання, а також того, до яких категорій персональних даних це відноситься. Деякі дані можуть потребувати додаткових заходів безпеки, ніж інші, або ізоляції від інших.
- Псевдонімізація — персональні дані та резервні копії/журнали слід псевдонімізувати як захід безпеки, щоб мінімізувати ризики потенційного порушення безпеки даних, наприклад, за допомогою хешування або шифрування.
- Резервне копіювання/журнали — збереження резервних копій та журналів в обсязі, необхідному для забезпечення інформаційної безпеки, використання аудиторських слідів та моніторингу подій як рутинного контролю безпеки. Вони мають бути захищені від несанкціонованого й випадкового доступу та зміни, регулярно переглядатися, а інциденти повинні обробляються оперативно.
- Відновлення після збоїв/безперервність роботи — необхідно враховувати вимоги щодо відновлення після збоїв та безперервності роботи інформаційних систем, щоб відновити доступність персональних даних після серйозних інцидентів.
- Захист відповідно до ризиків — усі категорії персональних даних повинні бути захищені заходами, пропорційними ризику порушення безпеки. Дані, що становлять особливий ризик, повинні, за можливості, зберігатися окремо від решти персональних даних.
- Управління реагуванням на інциденти безпеки — необхідно мати в наявності механізми, процедури та ресурси для виявлення, локалізації, обробки, звітування та навчання на прикладі порушення безпеки даних.
- Управління інцидентами — контролер повинен забезпечити процеси для обробки порушень та інцидентів, щоб зробити систему обробки більш надійною. Це включає процедури повідомлення, такі як управління повідомленнями (до наглядового органу) та інформуванням (суб'єктів даних).

Приклад

Контролер хоче вилучити велику кількість персональних даних з медичної бази даних, що містить електронні медичні картки (пацієнтів), на спеціальний сервер бази даних у компанії, щоб обробити вилучені дані з метою забезпечення якості. Компанія оцінила ризик для прав і свобод суб'єктів персональних даних, пов'язаний із розміщенням витягів на сервері, доступному для всіх працівників компанії, як високий. Оскільки в компанії є лише один відділ, який має обробляти витяги даних пацієнтів, контролер вирішив обмежити доступ до виділеного сервера лише працівниками цього відділу. Крім того, для подальшого зниження ризику, дані будуть псевдонімізовані перед передачею.

Щоб регулювати доступ і зменшити можливу шкоду від шкідливого програмного забезпечення, компанія вирішує розділити мережу та встановити контроль доступу до сервера. Крім того, вони встановлюють моніторинг безпеки, систему виявлення та запобігання вторгненням, а також ізолюють її від рутинного використання. Впроваджується автоматизована система аудиту для моніторингу доступу та змін. На основі цього генеруються звіти та автоматичні сповіщення про певні події, пов'язані з використанням, коли вони налаштовані. Контролер гарантує, що користувачі мають доступ лише за необхідності та з відповідним рівнем доступу. Неналежне використання можна швидко та легко виявити.

Деякі з витягів потрібно порівняти з новими витягами, і тому їх потрібно зберігати протягом трьох місяців. Контролер вирішує розмістити їх в окремих базах даних на одному сервері та використовувати для зберігання як прозоре шифрування, так і шифрування на рівні стовпців. Ключі для розшифрування даних стовпців зберігаються в спеціальних модулях безпеки, які може використовувати лише уповноважений персонал, але не вилучати.

Робота з майбутніми інцидентами робить систему більш стійкою та надійною. Контролер розуміє, що превентивні та ефективні заходи й гарантії повинні бути вбудовані в усі процеси обробки персональних даних, які він здійснює зараз і в майбутньому, і що це може допомогти запобігти майбутнім інцидентам порушення безпеки даних.

Контролер встановлює ці заходи безпеки як для забезпечення точності, цілісності та конфіденційності, так і для запобігання поширенню шкідливого програмного забезпечення в результаті кібератак, а також для забезпечення надійності рішення. Наявність надійних заходів безпеки сприяє зміцненню довіри із суб'єктами даних.

3.9 Підзвітність[41]

86. Принцип підзвітності передбачає, що контролер несе відповідальність за дотримання всіх вищезазначених принципів та має довести їх дотримання.

87. Контролер повинен довести дотримання принципів. При цьому контролер може продемонструвати наслідки заходів, вжитих для захисту прав суб'єктів даних, і чому ці заходи вважаються відповідними та ефективними. Наприклад, продемонструвати, чому той чи інший захід є доцільним для ефективного забезпечення принципу обмеження терміну зберігання.

88. Щоб мати можливість відповідально обробляти персональні дані, контролер повинен мати як знання, так і здатність забезпечувати захист даних. Це означає, що контролер повинен розуміти свої зобов'язання щодо захисту даних, передбачені GDPR, і бути здатним виконувати ці зобов'язання.

[41] Див. преамбулу 74, де контролери зобов'язані продемонструвати ефективність своїх заходів.

Прийнято

4 СТАТТЯ 25(3) СЕРТИФІКАЦІЯ

89. Згідно зі статтею 25(3), сертифікація відповідно до статті 42 може використовуватися як елемент для доведення відповідності принципам захисту даних за призначенням і за замовчуванням. І навпаки, документи, що доводять відповідність принципам захисту даних за призначенням і за замовчуванням, також можуть бути корисними в процесі сертифікації. Це означає, що якщо операція з обробки контролером або оператором була сертифікована відповідно до статті 42, наглядові органи повинні брати це до уваги при оцінці відповідності GDPR, зокрема, щодо принципів захисту даних за призначенням і за замовчуванням.

90. Якщо операція з обробки контролером або оператором сертифікована відповідно до статті 42, елементами, які сприяють доведенню відповідності статті 25(1) та (2), є процеси проектування, тобто процес визначення засобів обробки, управління, а також технічні та організаційні заходи для реалізації принципів захисту даних. Критерії сертифікації захисту даних визначаються органами сертифікації або власниками схем сертифікації, а потім затверджуються компетентним наглядовим органом або EDPB. Для отримання додаткової інформації про механізми сертифікації ми відсилаємо читача до Настанови EDPB щодо сертифікації[42] та інших відповідних керівництв, опублікованих на вебсайті EDPB.

91. Навіть якщо операція з обробки отримала сертифікацію відповідно до статті 42, контролер все одно несе відповідальність за постійний моніторинг та покращення відповідності критеріям захисту даних за призначенням і за замовчуванням, передбаченим статтею 25.

5 ЗАСТОСУВАННЯ СТАТТІ 25 ТА НАСЛІДКИ

92. Наглядові органи можуть оцінювати дотримання статті 25 відповідно до процедур, перелічених у статті 58. Коригувальні повноваження визначені у статті 58(2) і включають винесення попереджень, доган, розпоряджень про дотримання прав суб'єктів даних, обмеження або заборону обробки, адміністративні штрафи тощо.

93. Принципи захисту даних за призначенням і за замовчуванням також є фактором при визначенні рівня грошових санкцій за порушення GDPR, див. статтю 83(4).[43] [44]

---

[42] EDPB. «Настанови 1/2018 щодо сертифікації та визначення критеріїв сертифікації відповідно до статей 42 і 43 Регламенту». Версія 3.0, 4 червня 2019 року. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

[43] Стаття 83(2)(d) GDPR передбачає, що при визначенні накладення штрафів за порушення GDPR *«належна увага» повинна бути приділена «ступеню відповідальності контролера або оператора з урахуванням технічних та організаційних заходів, вжитих ними відповідно до статей 25 та 32».*

[44] Більше інформації про штрафи можна знайти в Робочій групі за статтею 29. «Настанови щодо застосування та встановлення адміністративних штрафів для цілей Регламенту 2016/679». РД 253, 3 жовтня 2017 року. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – схвалений EDPB.
Прийнято

6 РЕКОМЕНДАЦІЇ

94. Хоча це прямо не зазначено в статті 25, оператори та виробники також визнані ключовими учасниками механізму захисту даних за призначенням і за замовчуванням, вони повинні знати, що контролери зобов'язані обробляти персональні дані лише за допомогою систем і технологій, які мають вбудовані засоби захисту даних.

95. Здійснюючи обробку від імені контролерів або надаючи рішення контролерам, оператори та виробники повинні використовувати свій досвід для зміцнення довіри та орієнтувати своїх клієнтів, включаючи МСП, на розроблення/закупівлю рішень, які включають захист даних у процес обробки. Це, у свою чергу, означає, що розроблення продуктів і послуг має сприяти задоволенню потреб контролерів.

96. При виконанні статті 25 слід пам'ятати, що основною метою розроблення є *ефективна імплементація* принципів та *захисту* прав суб'єктів даних у відповідні заходи з обробки. Для того, щоб полегшити та покращити прийняття принципів захисту даних за призначенням і за замовчуванням, ми надаємо такі рекомендації контролерам, а також виробникам та операторам:

- Контролери повинні думати про захист даних на *початкових етапах* планування операції з обробки, ще до визначення засобів обробки.
- Якщо контролер має фахівця з питань захисту даних (DPO), EDPB заохочує активне залучення такого фахівця до інтеграції принципів захисту даних за призначенням і за замовчуванням у процедури закупівель та розроблення, а також у весь життєвий цикл обробки.
- Операція з обробки може бути *сертифікована.* Можливість сертифікувати операцію з обробки надає додаткову перевагу контролеру при виборі між різними програмними, апаратними засобами, послугами та/або системами від виробників або операторів. Тому виробники повинні прагнути доводити принципи захисту даних за призначенням і за замовчуванням протягом усього життєвого циклу розроблення рішення для обробки. Сертифікаційна печатка також може допомогти суб'єктам даних у виборі між різними товарами та послугами. Можливість сертифікувати обробку може слугувати конкурентною перевагою для виробників, операторів та контролерів, а також підвищує довіру суб'єктів даних до обробки їхніх персональних даних. Якщо сертифікація не пропонується, контролери повинні шукати інші *гарантії* того, що виробники або оператори дотримуються вимог захисту даних за призначенням і за замовчуванням.
- Контролери, оператори та виробники повинні враховувати свої зобов'язання щодо надання дітям до 18 років та іншим вразливим групам спеціального захисту при виконанні вимог захисту даних за призначенням і за замовчуванням.
- Виробники та оператори повинні прагнути сприяти впровадженню принципів захисту даних за призначенням і за замовчуванням, щоб підтримати здатність контролерів виконувати зобов'язання за статтею 25. З іншого боку, контролери не повинні обирати виробників або операторів, які не пропонують систем, що дозволяють або підтримують контролерів у дотриманні статті 25, оскільки контролери будуть нести відповідальність за її невиконання.
- Виробники та оператори повинні відігравати активну роль у забезпеченні дотримання критеріїв «сучасного рівня розвитку» та повідомляти контролерів про будь-які зміни в

«сучасному рівні розвитку», які можуть вплинути на ефективність запроваджених ними заходів. Контролери повинні включити цю вимогу як договірну умову, щоб бути впевненими, що вони завжди поінформовані.

- EDPB рекомендує контролерам вимагати, щоб виробники та оператори довели, як їхнє обладнання, програмне забезпечення, послуги або системи дозволяють контролеру дотримуватися вимог до підзвітності відповідно до принципів захисту даних за призначенням і за замовчуванням, наприклад, використовуючи ключові показники ефективності для доведення ефективності заходів та гарантій при реалізації принципів та прав.
- EDPB підкреслює необхідність гармонізованого підходу для ефективної реалізації принципів і прав та закликає асоціації або органи, які готують кодекси поведінки відповідно до статті 40, також включати в них галузеві настанови щодо захисту даних за призначенням і за замовчуванням.
- Контролери повинні бути справедливими щодо суб'єктів даних і прозорими щодо того, як вони оцінюють і доводять ефективне впровадження принципів захисту даних за призначенням і за замовчуванням, так само як контролери доводять дотримання GDPR відповідно до принципу підзвітності.
- Технології підвищення конфіденційності (PET), які досягли сучасного рівня розвитку, можуть застосовуватися як захід відповідно до вимог захисту даних за призначенням і за замовчуванням, якщо це доцільно в рамках підходу, заснованого на оцінці ризиків. PET самі по собі не обов'язково охоплюють зобов'язання, передбачені статтею 25. Контролери повинні оцінити, чи є цей захід доцільним та ефективним для реалізації принципів захисту даних та прав суб'єктів даних.
- Існуючі застарілі системи підпадають під ті ж зобов'язання щодо принципів захисту даних за призначенням і за замовчуванням, що й нові системи. Якщо застарілі системи ще не відповідають принципам захисту даних за призначенням і за замовчуванням, а зміни не можуть бути внесені для виконання зобов'язань, то застаріла система просто не відповідає зобов'язанням з GDPR і не може використовуватися для обробки персональних даних.
- Стаття 25 не знижує поріг вимог для МСП. Наступні пункти можуть полегшити дотримання МСП вимог статті 25:
    - Проведіть попередню оцінку ризиків
    - Почніть з невеликої обробки, а потім масштабуйте її обсяг і складність
    - Шукайте гарантії виробника та оператора щодо принципів захисту даних за призначенням і за замовчуванням, такі як сертифікація та дотримання кодексу поведінки
    - Використовуйте партнерів з хорошою репутацією
    - Поспілкуйтеся з органами із захисту даних (DPA)
    - Ознайомтеся з рекомендаціями органів із захисту даних та EDPB
    - Дотримуйтеся кодексів поведінки, якщо такі є
    - Отримайте професійну допомогу та консультації

Від імені Європейської ради із захисту даних

Голова

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

(Андреа Єлінек)

Прийнято