Дія: GDRP – що це і що передбачає:

написано Igor Krukovsky | 2026-03-25

Дата оновлення інформації : 05.01.2026, 16:19

GDPR (General Data Protection Regulation) – це загальний регламент Європейського Союзу про захист персональних даних, який встановлює єдині правила роботи з даними людей у цифровому та офлайн-середовищі. Його ключова ідея проста: **персональні дані належать людині, а не компанії, і бізнес може працювати з ними лише на чітко визначених, прозорих і законних умовах.**

Кого стосується GDPR?

GDPR застосовується не лише до компаній, зареєстрованих у ЄС. Регламент поширюється на будь-яку організацію у світі, якщо вона:

- пропонує товари або послуги людям, які перебувають у Європейському Союзі;
- або обробляє персональні дані таких осіб (наприклад, через сайт, аналітику, онлайн-сервіси чи маркетингові інструменти).

Тобто український бізнес також підпадає під дію GDPR, якщо працює з європейськими клієнтами, користувачами або партнерами.

Що вважається персональними даними?

GDPR трактує персональні дані дуже широко. Це будь-яка інформація, за якою людину можна ідентифікувати прямо або опосередковано. Йдеться не лише про ім’я чи електронну пошту, а й про:

- IP-адресу та онлайн-ідентифікатори;
- дані про місцеперебування;
- файли cookies;
- фото, біометричні дані;
- інформацію про здоров’я, релігійні переконання або політичні погляди.

Навіть псевдонімізовані дані можуть вважатися персональними, якщо особу реально ідентифікувати.

Основні ролі у GDPR

У межах GDPR чітко розрізняються ролі бізнесу в роботі з даними та роль людини, до якої ці дані належать. Це важливо, адже обов’язки компанії та права людини в регламенті не перетинаються, а доповнюють одне одного.

Зокрема:

- Суб’єкт даних — це фізична особа, персональні дані якої обробляються. У бізнес-контексті це клієнти, користувачі сайту, підписники розсилок або партнери.
- Контролер персональних даних — організація або особа, яка визначає, з якою метою та яким способом обробляються персональні дані. У більшості випадків контролером виступає сам бізнес.
- Процесор персональних даних — третя сторона, яка обробляє персональні дані від імені контролера та за його інструкціями. Це можуть бути хмарні сервіси, CRM-

системи, email-провайдери чи інші зовнішні підрядники.

Принципи обробки даних

GDPR вимагає, щоб будь-яка робота з персональними даними відповідала семи базовим принципам обробки, які фактично задають рамку для всіх рішень бізнесу у сфері даних:

- Законність, справедливість і прозорість. Дані можна обробляти лише на законних підставах, зрозуміло для людини та без прихованих цілей. Користувач має чітко розуміти, що відбувається з його даними.
- Чітко визначена мета. Персональні дані збираються лише для конкретних, чітко визначених цілей і не можуть використовуватися далі у спосіб, несумісний із цими цілями.
- Мінімізація даних. Бізнес має збирати тільки ті дані, які справді необхідні для заявленої мети, а не «про всяк випадок».
- Точність. Персональні дані повинні бути актуальними та коректними. Компанія має вживати заходів для виправлення або видалення неточних даних.
- Обмеження строку зберігання. Дані не можуть зберігатися довше, ніж це потрібно для досягнення мети обробки.
- Цілісність і конфіденційність. Дані мають бути захищені від несанкціонованого доступу, втрати або витоку за допомогою технічних і організаційних заходів безпеки.
- Підзвітність. Компанія не лише зобов’язана дотримуватися всіх принципів, а й бути готовою довести це — через документацію, процеси та внутрішні політики.

Коли бізнес має право обробляти

персональні дані?

GDPR виходить із презумпції заборони: якщо бізнес не може чітко пояснити, на якій правовій підставі він обробляє персональні дані, така обробка вважається незаконною.

Законні підстави визначені в статті 6 Регламенту і є вичерпними. Бізнес повинен обрати одну з них до початку збору даних і зафіксувати це у своїх процесах:

- **Згода суб'єкта даних.** Людина свідомо та однозначно погодилась на обробку своїх даних, наприклад підписалась на маркетингову розсилку або дала дозвіл на обробку даних у формі зворотного зв'язку.
- **Виконання договору або підготовка до нього.** Дані потрібні для надання послуги чи продажу товару: оформлення замовлення, доставка, виставлення рахунку, перевірка клієнта перед укладанням договору.
- **Виконання юридичного обов'язку.** Компанія зобов'язана обробляти дані відповідно до вимог законодавства, наприклад у сфері бухгалтерського обліку, податкової звітності або на вимогу суду.
- **Захист життєво важливих інтересів.** Обробка необхідна для захисту життя або здоров'я людини — цей пункт застосовується рідко, але є критичним у медичних або надзвичайних ситуаціях.
- **Виконання завдання в суспільних інтересах або здійснення офіційних повноважень.** Найчастіше стосується публічних або квазідержавних функцій, навіть якщо їх виконує приватна організація.
- **Законний інтерес компанії.** Найгнучкіша, але й найризикованіша підстава. Бізнес може обробляти дані, якщо має обґрунтований інтерес (наприклад, безпека, запобігання шахрайству), але права і свободи людини завжди мають пріоритет, особливо коли йдеться про дітей.

Важливо: обрану правову підставу потрібно зафіксувати документально і повідомити про неї людину. Якщо підстава змінюється, бізнес має обґрунтувати це і знову поінформувати особу.

Згода на обробку даних

GDPR суттєво підвищив вимоги до згоди. Вона має бути добровільною, конкретною, поінформованою та однозначною. Людина повинна легко зрозуміти, на що саме вона погоджується, і так само легко мати змогу відкликати згоду.

Окрема увага приділяється дітям: у більшості випадків особи до 13 років не можуть надавати згоду самостійно.

Ключові права суб’єктів даних на конфіденційність:

- Право бути поінформованим — людина має знати, які дані збираються та з якою метою.
- Право доступу — можливість отримати копію своїх даних і перевірити, як їх обробляють.
- Право на виправлення — можна вимагати, щоб неточні або неповні дані були скориговані.
- Право на видалення — у певних випадках людина може попросити стерти свої дані.
- Право на обмеження обробки — дозволяє тимчасово обмежити використання даних.
- Право на перенесення даних — можливість отримати свої дані у форматі, придатному для перенесення до іншого сервісу.
- Право на заперечення — можна заперечити проти обробки даних у маркетингових цілях або в інших визначених випадках.
- Права щодо автоматизованого прийняття рішень та профілювання — людина може обмежити або оскаржити використання даних для рішень, які приймаються без участі людини та можуть мати юридичні або значущі

наслідки.

Privacy by design і privacy by default

GDPR вимагає враховувати захист даних ще на етапі проєктування продуктів, сервісів і бізнес-процесів. Це означає, що питання приватності мають бути вбудовані в логіку рішень за замовчуванням, а не додаватися «потім».

Джерело: Дія Бізнес: https://business.diia.gov.ua/entrepreneur-handbook/item/gdpr

---

Далі поданий витяг з веб-сторінки European Commission

Правила для бізнесу та організацій

Дізнайтеся, що ваша організація повинна зробити для дотримання правил ЄС щодо захисту даних, і як ви можете допомогти громадянам реалізувати свої права згідно з цим регламентом.

Застосування регламенту

- Чи застосовуються правила захисту даних до даних про компанію?
- Чи застосовуються ці правила до малого та середнього бізнесу (МСП)?
- На кого поширюється закон про захист даних?

Робота з громадянами

- Чи існують обмеження на використання автоматизованого прийняття рішень?
- Чи можуть фізичні особи вимагати передачі своїх даних до іншої організації?
- Чи завжди ми повинні видаляти персональні дані, якщо людина просить про це?
- Як слід розглядати запити від осіб, які здійснюють свої права на захист даних?
- Що станеться, якщо хтось заперечить проти обробки моїх персональних даних моєю компанією?
- До яких персональних даних та інформації може отримати доступ особа за запитом?

Застосування та санкції

- Застосування
- Санкції

Правові підстави для обробки даних

- Чи існують якісь конкретні гарантії щодо даних про дітей?
- Чи можна використовувати дані, отримані від третьої сторони, для маркетингу?
- Підстави для обробки
- Конфіденційні дані

Бібліотека пов’язаних документів

Зобов’язання

- Чи зобов’язання однакові незалежно від обсягу даних, які обробляє моя компанія/організація?
- Контролер/обробник
- Спеціалісти із захисту даних
- Як я можу продемонструвати, що моя організація