

ERASMUS+ JEAN MONNET · ЦИКЛ ЛЕКЦІЙ

«Формування стратегії розвитку особистості в цифровому освітньому просторі:
Україна-ЄС»

№ 101127592 — FPDSDESUEU — ERASMUS-JMO-2023-HEI-TCH-RSCH



Тема 6

Конфіденційність і захист даних у Європейському Союзі: виклики та можливості для України



Лекція 6 з 7

План лекції

- 1** Приватність, конфіденційність і захист даних: взаємозв'язок понять
- 2** Персональні дані: визначення, ознаки та категорії; GDPR — обробка, підстави, принципи, права
- II** Завдання до теми 6: аудит персональних даних цифрового сервісу



01

ПИТАННЯ 1 3 2

Приватність, конфіденційність і захист даних: взаємозв'язок понять





Дані про людину в цифрових сервісах

Цифрові послуги дедалі частіше будуються навколо даних про людину.

Хто збирає і поєднує відомості

електронна ідентифікація мобільні застосунки
банківські сервіси соціальні мережі чат-боти
голосові помічники хмарні сховища відеоспостереження
системи штучного інтелекту



Що ці відомості дозволяють

розпізнати особу описати поведінку
інтереси зв'язки стан здоров'я
життєві обставини



Персональні дані як цифрова ідентичність

Персональні дані — не лише технічний ресурс організації. Вони відображають **цифрову ідентичність людини** та впливають на її:



автономію



репутацію



доступ до послуг



працевлаштування



кредитування



освіту



безпеку



Європейський підхід: обробка даних має **служити людині**, а не перетворювати її на пасивний об'єкт спостереження.



Подвійне значення теми для України

1



Цифровізація публічних послуг і бізнесу

Потребує **довіри громадян** до способів збирання та використання даних.

2



Євроінтеграція

Наближення законодавства, інституцій та практик до стандартів ЄС, зокрема:

незалежний нагляд

дієві права суб'єктів

належне управління ризиками



Мета захисту даних

Захист даних **не означає заборону** на їх використання.

Його мета — зробити обробку:

законною

прозорою

пропорційною

безпечною

**підконтрольною
людині**



Приватність, конфіденційність, захист даних

Поняття пов'язані, але **не тотожні**:



Приватність

Право людини на особисту сферу та контроль над втручанням у неї.



Конфіденційність

Режим нерозголошення інформації та обмеження доступу до неї.



Захист персональних даних

Ширша система правових, організаційних і технічних правил, що охоплює **весь життєвий цикл даних**.

збирання



...



видалення

02

ПИТАННЯ 2 3 2

Персональні дані: визначення, ознаки та категорії





Персональні дані: GDPR та закон України

ЄС · GDPR

Будь-яка інформація, що стосується фізичної особи, яку **ідентифіковано або можна ідентифікувати** прямо чи опосередковано.

Україна · Закон «Про захист персональних даних»

Відомості або сукупність відомостей про фізичну особу, яка **ідентифікована або може бути конкретно ідентифікована**.

🔗 Визначальним є не **формат інформації**, а можливість її **пов'язати з конкретною людиною**. Одна ознака іноді не дозволяє встановити особу, але поєднання кількох робить ідентифікацію реальною.

Форми даних:

текстова

числова

графічна

аудіо

відео

біометрична

Ознаки персональних даних



1



Зв'язок із фізичною особою

Інформація стосується людини, а не лише організації або абстрактного об'єкта.

2



Можливість ідентифікації

Пряма — за ім'ям, фото, номером документа; опосередкована — через комбінацію дати народження, місця роботи, адреси, поведінкових ознак, онлайн-ідентифікаторів.

3



Контекст обробки

Те саме значення може бути неперсональним в одному контексті й персональним в іншому, якщо організація має додаткові дані або засоби встановлення особи.

4



Структурований або автоматизований характер

GDPR охоплює автоматизовану обробку, а також неавтоматизовану, якщо дані входять або мають увійти до системи обліку.

Приклади персональних даних



Ідентифікаційні

ім'я, прізвище, дата народження, паспортні дані, РНОКПП, фото

Контактні

адреса, номер телефону, електронна пошта

Онлайн-ідентифікатори

IP-адреса, cookie, рекламний ідентифікатор пристрою, ідентифікатор облікового запису

Місцеперебування

дані про місцеперебування та маршрути

Професійні та інші

професійні, освітні, фінансові й поведінкові відомості

Голос і зображення

голос, зображення, відеозапис, історія звернень до сервісу

Чутливі

генетичні, біометричні дані та відомості про стан здоров'я

Тест: чи може організація або інший ймовірний користувач доступними засобами виділити конкретну людину з-поміж інших? Якщо так — це, найімовірніше, персональні дані.



Спеціальні категорії та вразливі дані

GDPR, стаття 9

Спеціальні категорії

Посилений режим. Обробка **загалом заборонена**, якщо не застосовується одна з виняткових підстав статті 9.

расове чи етнічне походження

політичні погляди

релігійні або світоглядні переконання

членство у профспілках

генетичні дані

біометричні дані для однозначної ідентифікації

дані про здоров'я

статеве життя або сексуальна орієнтація

Високий рівень обережності

Вразливі дані

Діти не виділені в окрему категорію статті 9, але потребують особливого захисту через меншу здатність усвідомлювати ризики та наслідки обробки.

Також — дані про:

соціальну вразливість

місце перебування військових

постраждалих від війни

ВПО

отримувачів допомоги

Конфіденційність і загальнодоступність



Персональні дані не можна довільно поширювати

Доступ надається визначеному колу осіб відповідно до мети й повноважень. Працівники зобов'язані не розголошувати дані, які стали їм відомі під час виконання обов'язків. Порушення режиму може спричинити **юридичну відповідальність**.



Але персональні дані не завжди секретні

Частина інформації може бути правомірно оприлюднена або відкрита за законом. Однак **загальнодоступність не скасовує статусу** персональних даних і не дає необмеженого права збирати їх у нові масиви, профілювати особу чи використовувати для несумісної мети.



Загальний регламент про захист даних

GDPR

Регламент (ЄС) 2016/679

Центральний акт ЄС щодо обробки персональних даних у приватному секторі та більшості сфер публічного управління.
Безпосередньо застосовується у державах-членах.

🔗 Два завдання

Високий рівень захисту фізичних осіб **та** вільний рух персональних даних у межах Союзу.

⚙️ Технологічна нейтральність

Вимоги залежать не від програми чи носія, а від факту, мети, масштабу і ризиків обробки.

🌐 Екстериторіальна дія (ст. 3)

Може поширюватися на організації за межами ЄС, якщо вони пропонують товари чи послуги особам у ЄС або відстежують їхню поведінку.

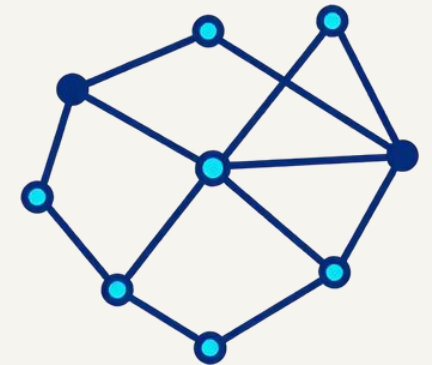
Що вважається обробкою

Обробка — будь-яка операція або сукупність операцій з персональними даними.

збирання реєстрація організація структурування зберігання адаптація або зміна пошук ознайомлення
використання розкриття шляхом передачі чи поширення зіставлення комбінування обмеження стирання знищення



Навіть **просте зберігання списку контактів** або **перегляд запису працівником** є обробкою.





Правові підстави обробки

Правомірність **не зводиться лише до згоди**. Для кожної мети контролер визначає підставу **до початку обробки** і не підмінює її після виникнення спору.

1	Згода	Вільна, конкретна, поінформована й однозначна воля особи; її можна відкликати так само легко, як надати.
2	Договір	Обробка необхідна для виконання договору із суб'єктом або для дій на його запит до укладення договору.
3	Юридичний обов'язок	Контролер обробляє дані, щоб виконати вимогу права ЄС або держави-члена.
4	Життєво важливі інтереси	Захист життя чи здоров'я особи, коли інша підстава непридатна.
5	Суспільний інтерес або офіційні повноваження	Типова підстава для органів публічної влади за наявності чіткої правової норми.
6	Законний інтерес	Після балансування інтересу контролера з правами людини; не застосовується органами влади під час виконання публічних завдань.



Мета → дані → підстава

ПРАКТИЧНЕ ПРАВИЛО

1. Сформулюйте конкретну мету



2. Визначте мінімально необхідні дані



3. Лише після цього — правову підставу



Формула «**зберемо** про всяк випадок, а мету знайдемо пізніше» суперечить логіці GDPR.



Ключові принципи GDPR

1	Законність, справедливість і прозорість	Людина розуміє, хто, навіщо, на якій підставі та як використовує її дані; обробка не повинна бути оманливою чи несподівано шкідливою.
2	Обмеження мети	Дані збирають для конкретних, чітких і законних цілей; подальше використання не повинно бути несумісним із ними.
3	Мінімізація даних	Обробляються лише адекватні, релевантні й необхідні відомості.
4	Точність	Неточні дані виправляють або видаляють без невиправданої затримки.
5	Обмеження зберігання	Дані у формі, що дозволяє ідентифікацію, зберігаються не довше, ніж потрібно для мети.
6	Цілісність і конфіденційність	Належний рівень безпеки від незаконної обробки, випадкової втрати, знищення або пошкодження.
7	Підзвітність	Контролер може довести дотримання принципів: політики, записи, оцінювання ризиків, договори, аудити, навчання.



Права суб'єктів персональних даних

Реалізація права залежить від підстави та обставин обробки: наприклад, право на видалення не є абсолютним, якщо закон вимагає зберігати дані.

1	Право бути поінформованим ст. 13–14	Зрозуміла інформація про контролера, цілі, підстави, одержувачів, строки, передачі та права.
2	Право на доступ ст. 15	З'ясувати, чи обробляються дані, й отримати доступ до них та пов'язаної інформації.
3	Право на виправлення ст. 16	Неточні відомості підлягають виправленню, а неповні — доповненню.
4	Право на видалення ст. 17	За визначених умов — вимагати стирання даних («право на забуття»).
5	Право на обмеження обробки ст. 18	Дані тимчасово зберігають без активного використання, поки вирішується спір або перевіряється законність.



Права суб'єктів персональних даних

6	Право на портативність ст. 20	Дані у структурованому, поширеному й машинозчитуваному форматі.
7	Право на заперечення ст. 21	Проти обробки на підставі суспільного або законного інтересу; проти прямого маркетингу — у будь-який момент.
8	Права щодо автоматизованих рішень і профілювання ст. 22	Гарантії щодо рішень, прийнятих виключно автоматизовано, з юридичними або подібно значущими наслідками.
9	Право на скаргу й судовий захист ст. 77–79	Звернення до наглядового органу та суду.



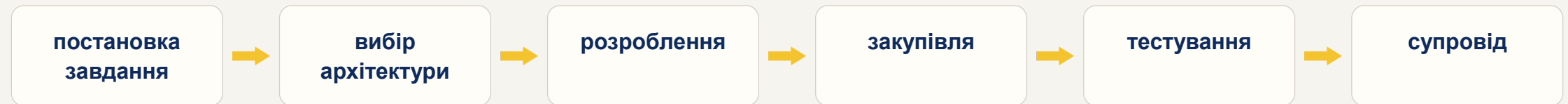
Типові цифрові ситуації захисту даних

	Інтернет речей	Фітнес-браслети, датчики й «розумний будинок» формують поведінкові та іноді медичні профілі.
	Відеоспостереження	Камери збирають зображення, час і місце; розпізнавання обличчя додає біометричний ризик.
	Мобільні застосунки	Доступ до контактів, геолокації, фото й сенсорів має відповідати реальній функції сервісу.
	Чат-боти, голосові помічники та ШІ	Текст, голос, контекст, історія взаємодії; увага до прозорості й вторинного використання для навчання моделей.
	Реєстрація та авторизація	Облікові записи, журнали входу, e-mail і багатофакторна автентифікація — частина системи захисту.
	Хмарні сервіси	Місце зберігання, субпроцесори, транскордонна передача, повернення і видалення даних.
	Публічні реєстри й е-послуги	Законна публічна функція не скасовує вимог мінімізації, розмежування доступу та безпеки.



Конфіденційність за проектом і за замовчуванням

Захист даних вбудовується в сервіс на всіх етапах:



Privacy by design

Конфіденційність за проектом: ризики приватності враховуються **в усіх рішеннях** про продукт або процес.



Privacy by default

Конфіденційність за замовчуванням:

мінімальний обсяг даних

мінімально потрібне коло осіб з доступом

обмежені строки зберігання

Кібербезпека ≠ відповідність GDPR



Безпека інформації

Захищає

конфіденційність

цілісність

доступність



Захист персональних даних

Додатково вимагає

правомірної мети

мінімізації

прозорості

реалізації прав

підзвітності



Кібербезпека є необхідною, але недостатньою умовою відповідності GDPR.

Завдання до теми 6: аудит персональних даних цифрового сервісу



Мета: навчитися розпізнавати персональні дані, визначати мету й правову підставу обробки, перевіряти дотримання принципів GDPR та пропонувати заходи privacy by design і privacy by default.

Оберіть сервіс:

мобільний застосунок

чат-бот

електронна послуга

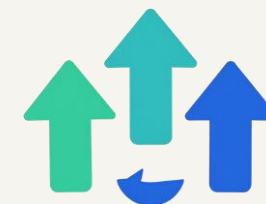
система дистанційного навчання

сервіс доставки

програма лояльності

вигаданий аналог

Сім кроків аудиту



1	Об'єкт аналізу	Коротко опишіть призначення сервісу, його користувачів і одну основну операцію з даними.
2	Інвентаризація	Визначте щонайменше шість категорій даних, їх джерело, мету та необхідність. Не копіюйте реальні дані користувачів.
3	Ролі та підстава	Визначте суб'єкта, контролера, процесора/оператора, одержувачів і DPO або відповідальну особу; для кожної мети — правову підставу.
4	Перевірка принципів	Знайдіть щонайменше три невідповідності принципам GDPR: надмірні поля, нечітка мета, занадто великий строк, непрозоре повідомлення, надмірний доступ тощо.
5	Права людини	Оберіть три права суб'єкта даних і поясніть, як сервіс повинен забезпечити їх реалізацію.
6	Редизайн приватності	Запропонуйте п'ять конкретних змін: щонайменше дві організаційні й дві технічні.
7	Підсумок	Висновок у 4–5 реченнях: чи є обробка пропорційною меті та що потрібно змінити насамперед.



Інвентаризація персональних даних

Обраний сервіс:

Основна функція:

№	Категорія даних	Джерело	Мета обробки
1			
2			
3			
4			
5			
6			



Принципи, права та дії

Принцип / право	Виявлена проблема або спосіб реалізації	Запропонована дія

Підсумковий висновок:

Джерела до теми

1

Закон України «Про захист персональних даних»

zakon.rada.gov.ua/laws/show/2297-17

2

Регламент (ЄС) 2016/679 (GDPR) — офіційний переклад

zakon.rada.gov.ua/laws/show/984_008-16



ТЕМА 6 · ЗАВЕРШЕННЯ

Дякую за увагу!

Наступна лекція: Тема 7 · Створіть свій Europass: можливості
працевлаштування та навчання в ЄС



Erasmus+ Jean Monnet · «Формування стратегії розвитку особистості в цифровому освітньому просторі: Україна-ЄС» · № 101127592 — FPDSDESUEU
— ERASMUS-JMO-2023-HEI-TCH-RSCH



Проект № 101127592 — FPDSDESUEU фінансується Європейським Союзом. Однак висловлені погляди та думки належать лише автору(ам) і не обов'язково відображають погляди Європейського Союзу або Європейського виконавчого агентства з питань освіти та культури (EACEA). Ні Європейський Союз, ні EACEA не несуть за них відповідальності.