Автор тренінгу Ігор Афонін

Захист персональних даних

Про автора

Ігор експерт у сфері інформаційної безпеки та більш ніж 20 років досвіду роботи в цьому напрямку. За роки роботи у цій сфері займався побудовою системи управління інформаційної безпеки відповідно до вимог міжнародного стандарту ISO/IEC 27000 . Маю значний досвід впровадження різних систем інформаційної безпеки(WAF, IPS, IDS, EDR, PAM, DLP, AD, IAM, Azure AD, Microsoft Zero Trust, PAW).

https://www.linkedin.com/in/igor-afonin-3254665/

eAdvise

Основні визначення

Персональні дані
– це будь-яка інформація, що стосується конкретної фізичної особи, ідентифікованої або такої, що може бути ідентифікована. Це інформація, яка дозволяє прямо або опосередковано визначити особу.

eAdvise

Основні категорії персональних даних

1. **Основні ідентифікаційні дані:**
   - Ім'я, прізвище, по-батькові
   - Дата і місце народження
   - Ідентифікаційний код, номер паспорта або іншого посвідчення особи

eAdvise

Основні категорії персональних даних

2.Контактна інформація:

- Адреса проживання
- Номер телефону
- Електронна пошта

eAdvise

Основні категорії персональних даних

3.Фінансова інформація:

- Банківські реквізити
- Інформація про доходи та витрати

eAdvise

Основні категорії персональних даних

4.Цифрові ідентифікатори:

- IP-адреса, файли cookie
- MAC-адреса пристрою
- Данні про активність у соціальних мережах, інші дані, що пов’язані з онлайн-ідентичністю

eAdvise

Основні категорії персональних даних

5.Особисті характеристики:

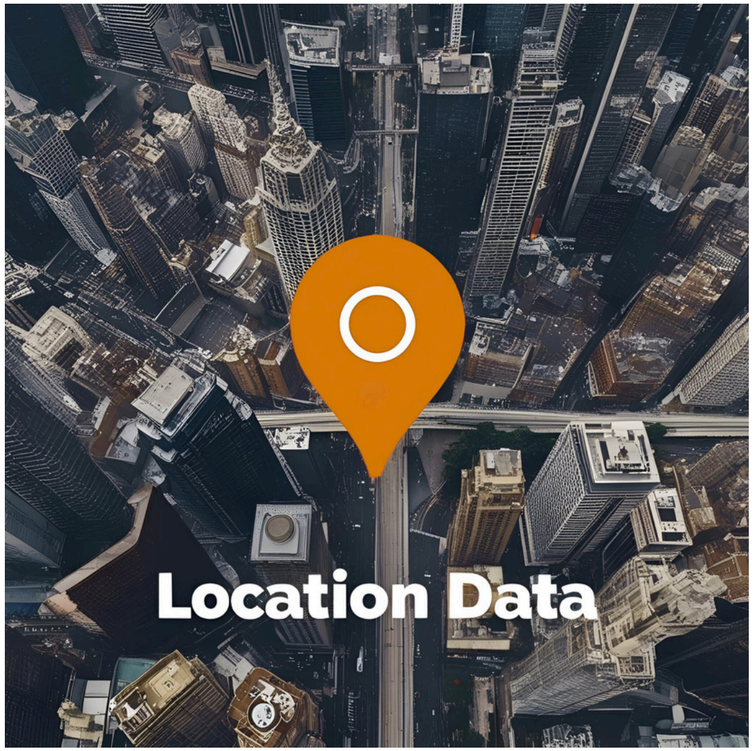
- Генетичні дані, біометричні дані (відбитки пальців, скан сітківки ока)
- Медичні дані (діагнози, історія хвороби)
- Дані про расу, релігійні переконання, політичні погляди, сексуальну орієнтацію.

eAdvise

Основні категорії персональних даних

6.Дані про місцезнаходження:

- Геолокація або історія місцезнаходження, що збирається за допомогою GPS на мобільних пристроях або інших технологій.



eAdvise

Важливість захисту персональних даних

Персональні дані є важливим об’єктом для захисту, оскільки їх витік або неправильне використання може призвести до порушення конфіденційності людини, викрадення її особистості, фінансових втрат або навіть дискримінації.

eAdvise

Важливість захисту персональних даних

Дотримання вимог захисту персональних данних регулюєтся на законодавчому рівні. В Україні це: **Закон України "Про захист персональних даних" та GDPR (Загальний регламент захисту даних) в Європейському Союзі.**

Ці закони регулюють, як персональні дані повинні збиратися, зберігатися та використовуватися, щоб забезпечити конфіденційність та права користувачів.

eAdvise

Важливість захисту персональних даних

Значення захисту особистих даних для користувачів:

- **Конфіденційність та приватність:** Користувачі мають право на захист своєї особистої інформації від неправомірного доступу та використання. Захищені дані дозволяють їм відчувати себе безпечно та захищено в онлайн та офлайн середовищі.
- **Довіра до сервісів та платформ:** Користувачі звертають увагу на захист персональних даних, коли вони вибирають сервіси та платформи для використання. Правильне та ефективне керування їхніми даними підвищує довіру та відображається на репутації компаній.
- **Запобігання кіберзлочинності:** Зловмисники можуть використовувати незахищені персональні дані для шахрайства, крадіжок ідентичності, фішингу та інших кіберзлочинних активностей. Захищені дані зменшують ризик стати жертвою таких атак.

eAdvise

Важливість захисту персональних даних

Значення захисту особистих даних для організацій:

- **Відповідність законодавству:** Організації зобов'язані дотримуватися законодавства з приводу захисту персональних даних, такого як GDPR чи HIPAA. Невиконання цих вимог може призвести до серйозних штрафів та правових наслідків.
- **Збереження довіри клієнтів:** Клієнти та клієнтська база є найціннішим активом для багатьох компаній. Захист персональних даних свідчить про те, що організація пильно ставиться до конфіденційності своїх клієнтів, що підвищує рівень довіри.
- **Зменшення ризиків:** Ефективне керування та захист персональних даних допомагає зменшити ризики порушення безпеки даних, крадіжки ідентичності та інших кіберзагроз, що може призвести до великих фінансових та репутаційних втрат.
- **Збільшення ефективності:** Добре організований захист персональних даних сприяє створенню порядку та ефективності в процесах обробки даних організації, що в свою чергу підвищує продуктивність та забезпечує безпеку бізнесу.

eAdvise

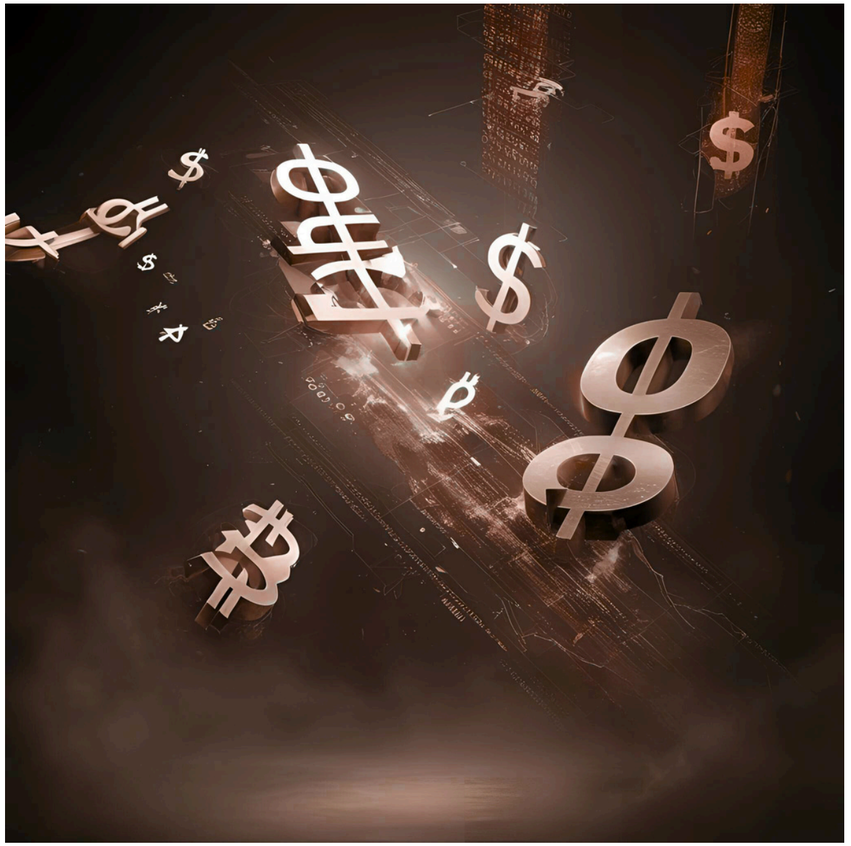
Сценарії використання персональних даних

Крадіжка ідентичності: Зловмисники можуть використовувати персональні дані, такі як ім'я, адреса, номери соціального страхування тощо, для видачі себе за іншу особу та відкриття кредитних рахунків, отримання кредитів або навіть здійснення медичних послуг.

eAdvise

Сценарії використання персональних даних

Фінансові шахрайства:
Зловмисники можуть використовувати фінансові дані, такі як номери кредитних карток або банківські реквізити, для здійснення несанкціонованих транзакцій або викрадення грошей з банківських рахунків.



eAdvise

Сценарії використання персональних даних

Спам та фішинг:
Зловмисники можуть використовувати електронну адресу та інші контактні дані для надсилання спаму, фішингових повідомлень або шкідливого програмного забезпечення з метою шахрайства або шпигунства.

eAdvise

Сценарії використання персональних даних

Соціальна інженерія: Зловмисники можуть використовувати зібрані персональні дані для маніпулювання людьми та отримання конфіденційної інформації або доступу до захищених систем.

eAdvise

Сценарії використання персональних даних

Фізична небезпека:
У випадках, коли зловмисники збирають геолокаційні дані або іншу особисту інформацію, вони можуть використовувати цю інформацію для стеження за жертвами, вчинення на їх адресу злочинів або навіть для шантажу.

eAdvise

GDPR (Загальний регламент з захисту даних)

- **Сфера діяльності: GDPR (General Data Protection Regulation)** застосовується до всіх організацій, які обробляють персональні дані громадян Європейського Союзу, незалежно від місцезнаходження цих організацій.
- **Потреба: GDPR** встановлює правила та стандарти щодо обробки, збереження та захисту персональних даних, забезпечуючи права та конфіденційність даних громадян.

eAdvise

Основні принципи: GDPR

1.Законність, справедливість і прозорість (Lawfulness, Fairness, and Transparency): Обробка персональних даних повинна бути законною, справедливою та прозорою для суб'єкта даних. Це означає, що організації мають чітко і відкрито інформувати людей про те, як їхні дані збираються, використовуються та зберігаються.

eAdvise

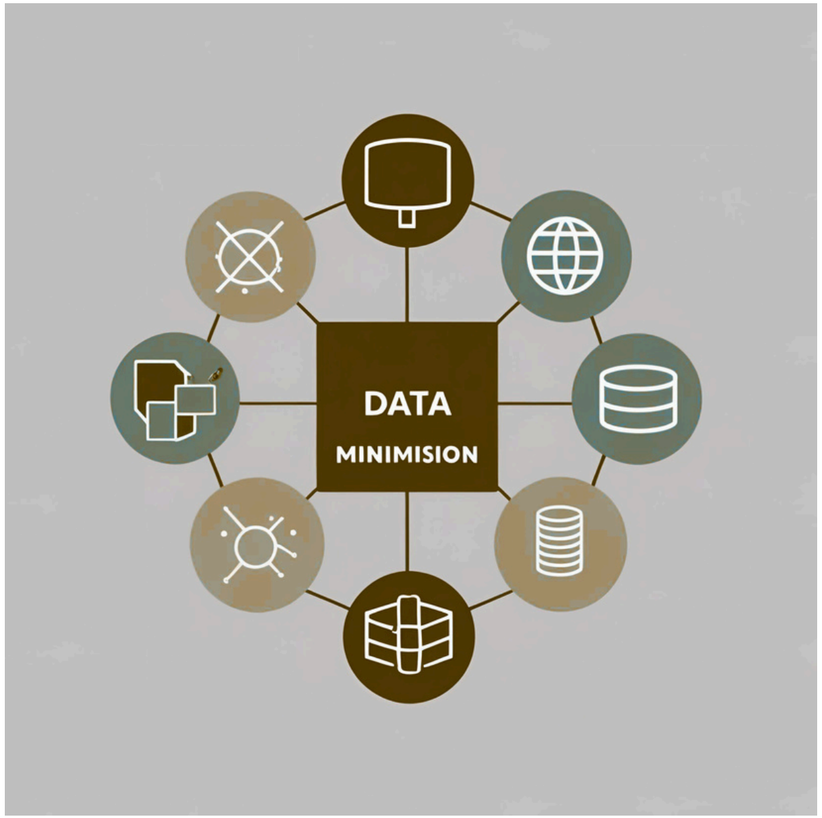
Основні принципи: GDPR

2.Обмеження мети (Purpose Limitation): Персональні дані можуть збиратися лише з конкретною, чітко визначеною і законною метою. Дані не можуть бути використані для інших цілей, несумісних з початковою, без додаткової згоди суб'єкта даних.

eAdvise

Основні принципи: GDPR

3.Мінімізація даних (Data Minimization): Організації повинні збирати тільки ті персональні дані, які є необхідними для досягнення конкретної мети. Збирання надлишкових даних заборонено, що допомагає знизити ризик зловживання даними.



eAdvise

Основні принципи: GDPR

4.Точність (Accuracy): Персональні дані мають бути точними, повними та актуальними. Організації зобов'язані вживати всіх розумних заходів для видалення або виправлення неточних даних.

eAdvise

Основні принципи: GDPR

5.Обмеження зберігання (Storage Limitation): Персональні дані не повинні зберігатися довше, ніж це необхідно для досягнення мети, з якою вони були зібрані. Після досягнення мети дані мають бути видалені або анонімізовані, за винятком випадків, коли збереження необхідне згідно з законодавством.

eAdvise

Основні принципи: GDPR

6.Цілісність і конфіденційність (Integrity and Confidentiality): Організація зобов'язана забезпечити належний захист персональних даних, включаючи технічні та організаційні заходи для захисту від несанкціонованого доступу, обробки або втрати даних. Це включає використання засобів шифрування, контролю доступу та інших технологій безпеки.

eAdvise

Основні принципи: GDPR

7.Підзвітність (Accountability):
Організації несуть відповідальність за дотримання всіх принципів GDPR і повинні бути готові продемонструвати це. Це означає, що компанії повинні документувати всі процеси обробки даних, впроваджувати політики захисту даних і мати можливість довести свою відповідність регламенту у разі перевірки.

eAdvise

Інші важливі положення GDPR

1.Права суб’єктів даних: GDPR надає громадянам ЄС певні права щодо їхніх персональних даних, зокрема право на доступ, виправлення, видалення ("право бути забутим"), обмеження обробки, право на перенесення даних і право заперечувати проти обробки.

2.Згода: Для обробки персональних даних необхідно отримати чітку згоду суб'єкта даних, причому згода повинна бути добровільною, конкретною, інформованою і однозначною.

3.Звітування про порушення безпеки: У випадку витоку або порушення безпеки персональних даних організації зобов'язані повідомити наглядові органи протягом 72 годин та інформувати постраждалих осіб, якщо порушення несе загрозу їх правам і свободам.

4.Підвищені штрафи: GDPR передбачає високі штрафи за порушення регламенту, які можуть досягати 20 мільйонів євро або 4% від світового річного обороту компанії, залежно від того, що більше.

eAdvise

Для комунікації

НАШ ВЕБ-САЙТ

НАШ LINKEDIN

@EADVISE_HUB

eAdvise