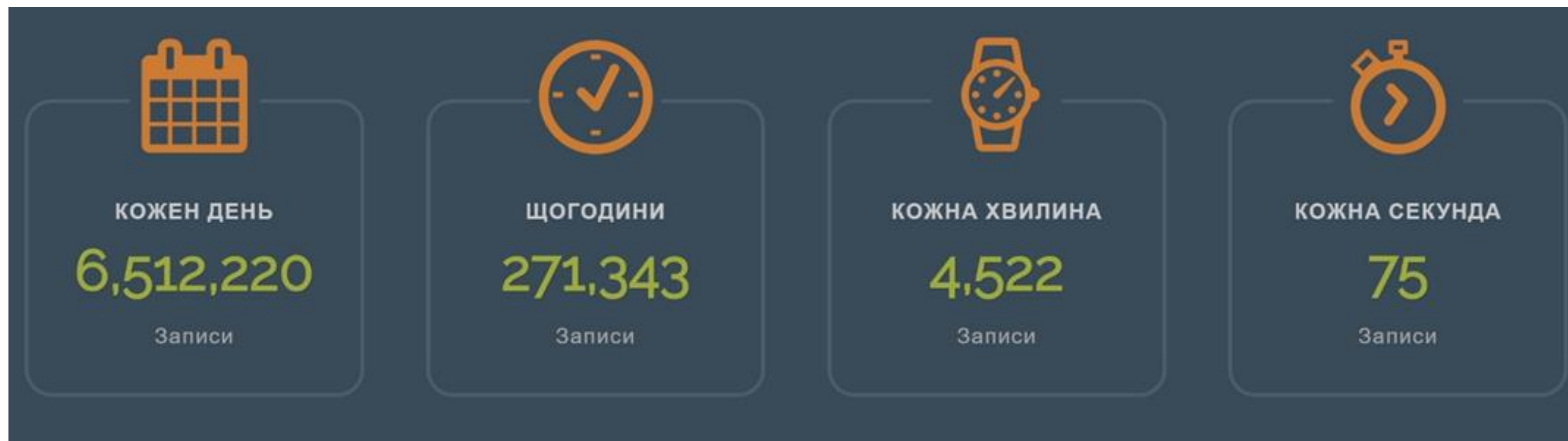


GDPR compliance

Опанас Карлін
Партнер ESQUIRES, адвокат



СТАТИСТИКА ПОРУШЕННЯ ДАНИХ У СВІТІ DATA BREACH STATISTICS



В Україні 25,5млн. записів викрадені або зламані

За даними <https://breachlevelindex.com/>

До 70% кібератак використовують комбінацію техніки фішингу та хакерства і залучають другорядну жертву.

«Звіт про розслідування порушень даних за 2015 рік» | Verizon

74% CISOs стурбовані тим, що співробітники крадуть чутливу інформацію про компанію.

«Опитування SANS 2015 про загрози інсайдерам» | SpectorSoft

Кіберзлочинність до 2019 року обійдеться підприємствам понад \$ 2 трлн.

*[https://www.juniperresearch.com/press/press-releases/
cybercrime-cost-businesses-over-2trillion](https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion)*



Стосується персональних даних не лише громадян ЄС, а всіх осіб, що знаходяться на території ЄС

GDPR
General Data Protection
Regulation
Загальний регламент про
захист даних

почав застосовуватися 25 травня 2018 року

не вимагає від національних урядів прийняття законів, які уможливлють його дію (є безпосередньо зобов'язальним і застосовним)

застосовується до:

- контролерів, операторів, суб'єктів даних, розташованих у ЄС
- організації, що базуються за межами ЄС, якщо вони збирають чи опрацьовують особисті дані фізичних осіб, розташованих в межах ЄС

Ключові терміни



«Персональні дані»

будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати



«Суб'єкт даних»

фізична особа, яку можна ідентифікувати, зокрема, за такими ідентифікаторами як

- ім'я, ідентифікаційний номер,
- дані про місцеперебування,
- онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.



«Опрацювання даних»

означає будь-яку операцію або низку операцій з персональними даними:

- збирання, реєстрація, організація;
- структурування;
- зберігання;
- адаптація чи зміна;
- пошук;
- ознайомлення;
- використання;
- розкриття через передавання;
- розповсюдження чи надання іншим чином;
- упорядкування чи комбінування;
- обмеження;
- стирання чи знищення.



«Контролер даних» (Data Controller)

фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних.



«Порушення захисту даних»

порушення безпеки, що призводить до випадкового чи незаконного **знищення, втрати, зміни, несанкціонованого розкриття або доступу** до персональних даних, які передано, збережено або іншим чином опрацьовано.



«Оператор даних» (Data Processor)

фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера.



«Згода суб'єкта даних»

вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних.

НАГЛЯД:

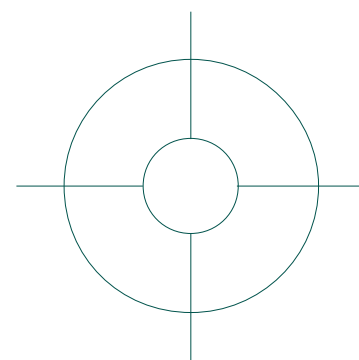
Європейська Комісія

Європейська рада із захисту даних (входять голови всіх наглядових органів)

Наглядові органи
(у кожній країні ЄС – свій)

Керівний наглядовий орган
– за місцем знаходження контролера/оператора

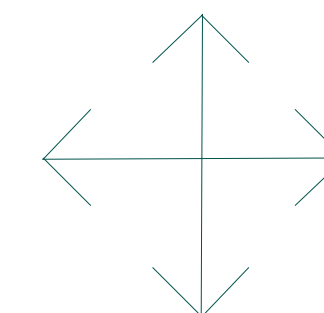
КРИТЕРІЇ ЗАСТОСОВНОСТІ:



МІСЦЕЗНАХОДЖЕННЯ

Знаходження контролера або оператора на території ЄС

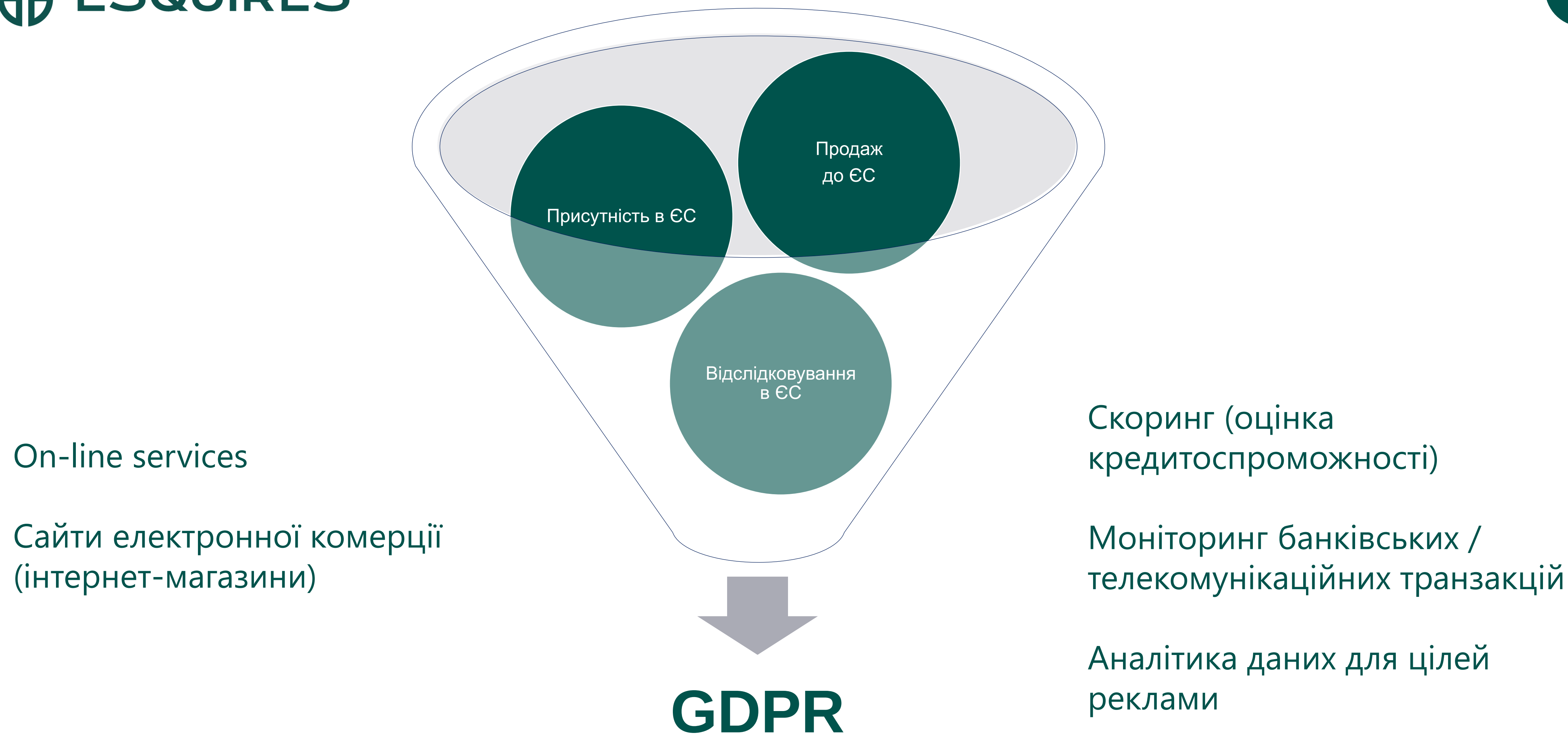
(відділення/філія, представництво, дочірня компанія зі статусом юридичної особи).



СПРЯМУВАННЯ ДІЯЛЬНОСТІ

Знаходження контролера або оператора поза межами території ЄС, якщо опрацювання даних пов'язано з:

- постачанням товарів/наданням послуг (платним або безоплатним) суб'єктам даних у ЄС;
або
- моніторингом поведінки суб'єктів даних, якщо така поведінка має місце у межах ЄС.





ВІДПОВІДАЛЬНІСТЬ

Ключові повноваження Наглядового органу

СЛІДЧІ ПОВНОВАЖЕННЯ

- видавати розпорядження надати будь-яку інформацію, яку він вимагає для виконання своїх завдань;
- проводити розслідування в формі перевірок захисту даних;
- здійснювати перегляд сертифікацій;
- повідомляти про передбачуване порушення Регламенту;
- доступ до всіх персональних даних і до всієї інформації, необхідної для виконання його завдань;
- доступ до будь-яких приміщень та/або будь-якого обладнання і засобів опрацювання даних контролера і оператора.

ВИПРАВНІ ПОВНОВАЖЕННЯ

- надсилати **попередження** контролеру або оператору про те, що призначені операції опрацювання ймовірно порушать положення Регламенту;
- виносити **догану** контролеру або оператору, якщо операції опрацювання порушують положення Регламенту;
- накладати тимчасове чи остаточне обмеження, в тому числі, **заборону, на опрацювання**;
- **накладати адміністративні штрафи**, залежно від обставин кожної індивідуальної справи; наказувати **призупинення потоків даних** до одержувача в третій країні чи до міжнародної організації.

ШТРАФНІ САНКЦІЇ ВЕРХНЬОЇ МЕЖІ

до **4% річного обороту** або
до **20 мільйонів євро**
(в залежності від того, яка з сум більша)

накладаються за **суттєві** порушення:

- основних принципів обробки даних, в тому числі щодо надання згоди (статті 5–7, 9);
- прав суб'єктів даних (статті 12–22);
- положень про передавання даних (статті 44–49);
- права на самовираження й інформацію, щодо збирання національних ідентифікаційних номерів, процедур працевлаштування, щодо нерозголошення таємниць і правил захисту даних для церков і релігійних організацій.

ШТРАФНІ САНКЦІЇ НИЖНЬОЇ МЕЖІ

до **2% річного обороту** або
до **10 мільйонів євро**
(в залежності від того, яка з сум більша)

накладаються за **не суттєві** порушення:

- отримання згоди дитини відповідно до чинних умов стосовно послуг цифрового суспільства (ст. 8);
- інформування наглядового органу про порушення персональних даних (ст. 33).
- інформування суб'єкта даних про порушення персональних даних (ст. 34).
- призначення співробітника з питань захисту даних (статті 37–39).



50 млн. євро

порушення зобов'язань
прозорості й поінформованості та
порушення зобов'язання мати
законну підставу для
опрацювання даних із метою
персоналізації реклами



500 тис. фунтів

надання розробникам
застосунків доступу до
інформації про 87 млн.
користувачів без достатньої
їх згоди

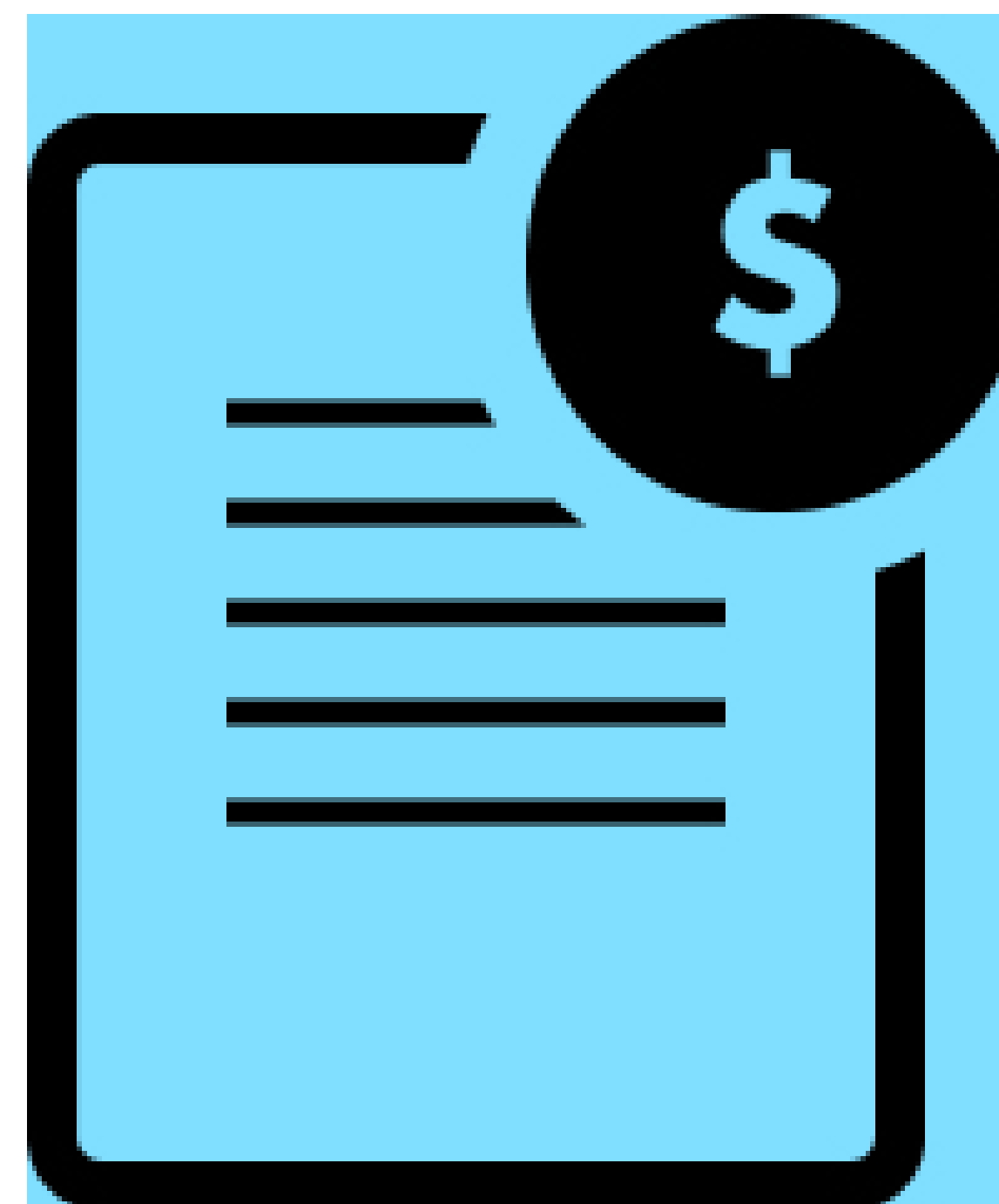


розслідування триває

не вжиття запобіжних заходів
щодо захисту конфіденційності
даних клієнтів (витік даних
щодо 380 тис. фінансових
транзакцій, які торкнулися 244
тис. кредитних карток)

Обставини, що враховуються Наглядним органом при застосуванні штрафних санкцій

- специфіка, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм;
- навмисний або недбалий характер порушення;
- будь-які дії, вжиті заходи для зниження рівня шкоди, заподіяної суб'єктами даних;
- ступінь відповідальності контролера або оператора, зважаючи на технічні та організаційні інструменти, які вони застосовують;
- категорії персональних даних, на які вплинуло порушення;
- дотримання затверджених кодексів поведінки;
- рівень співпраці з наглядним органом для відшкодування порушення і скорочення можливих негативних наслідків порушення.





КОНТРОЛЕРУ, ЩО ДОПУСТИВ ПОРУШЕННЯ ЗАГРОЖУЮТЬ:

- **Відшкодування шкоди** (суб'єкту даних)
- **Штраф**
- **Санкції** (їх можуть вводити країни ЄС)

GDPR compliance – це система контролю та управління ризиками, які можуть виникнути через недотримання умов GDPR.

Відповідно до умов GDPR, компанії, установи, організації не тільки повинні забезпечити, щоб персональні дані були зібрані на законних підставах і під жорсткими умовами, а й зобов'язані захищати їх від зловживання та експлуатації, а також поважати права власників даних – або їм загрожує покарання за це.





ЩОДО СУБ'ЄКТА ДАНИХ

Надання / відкликання згоди
Надання інформації (у момент збору даних)
Доступ до своїх персональних даних
Виправлення (неточної/недостовірної інформації)
Видалення («право бути забутим»)
Обмеження обробки даних
Мобільність (перенесення) даних
Право на заперечення
Захист даних за призначенням і за замовчуванням

Повідомити про порушення захисту персональних даних (якщо це ймовірно призведе до виникнення високого ризику для прав і свобод фізичних осіб)

ЩОДО НАГЛЯДОВОГО ОРГАНУ

Записувати діяльність з обробки даних (контролер і оператор повинні вести облік діяльності з обробки, облік усіх категорій обробки і надати ці відомості на запит наглядового органу).

Співробітничати

Оцінювати вплив на захист даних і надавати попередні консультації

Пройти добровільну сертифікацію (до 3 років)

Повідомити про порушення захисту персональних даних (якщо таке порушення навряд чи призведе до виникнення ризику для прав і свобод фізичних осіб)



ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ПРАВ:

Надання / відкликання згоди (на обробку персональних даних)

- очевидне та однаково легке

Надання інформації (у момент збору даних) суб'єкту даних про:

- контролера;
- контактні дані посадової особи, яка займається питаннями захисту даних;
- цілі обробки даних...

Доступ до своїх персональних даних

- контролер надає копію персональних даних, що підлягають обробці;
- інформування про обсяг і спосіб обробки (наприклад, у розділі «КОНФІДЕНЦІЙНІСТЬ»)



Виправлення (неточної/недостовірної інформації)

Видалення («право бути забутим»)

- за запитом суб'єкта даних;
- автоматично (відсутність потреби, відкликання згоди, закінчення строків).

Обмеження обробки даних
(застереження при наданні згоди)

Мобільність (перенесення) даних
можливість передавати зібрані персональні дані іншій особі (іншому контролеру)

Право на заперечення

(коли персональні дані обробляються для прямих маркетингових цілей (профайлінг), суб'єкт даних має право у будь-який час оскаржити обробку персональних даних у цій частині)

- дозволяти користувачеві в будь-який час просити припинити обробку своїх особистих даних, якщо така обробка не вимагається законом;
- спеціально припинити використання для маркетингових комунікацій;
- чітко інформувати користувача про його права на обробку даних.

Захист даних за призначенням і за замовчуванням

- використання псевдонімів, призначених для результативної реалізації принципів захисту даних, зокрема, мінімізації даних;
- за замовчуванням опрацьовують лише ті персональні дані, які є необхідними для кожної спеціальної цілі опрацювання.

Право не підлягати рішенню, що ґрунтується винятково на автоматизованому опрацюванні, в тому числі, профайлінгу



НІЯКИХ «ЗІРОЧОК» І МІКРОШРИФТУ?

Контролер повинен забезпечити надання будь-якої інформації суб'єкту даних у **стислій, прозорій, доступній для розуміння та легко доступній формі**, з використанням чітких і простих формулювань, зокрема, для будь-якої інформації, яку спеціально призначено для дитини.

Повідомлення
Розслідування
Припинення
Вдосконалення



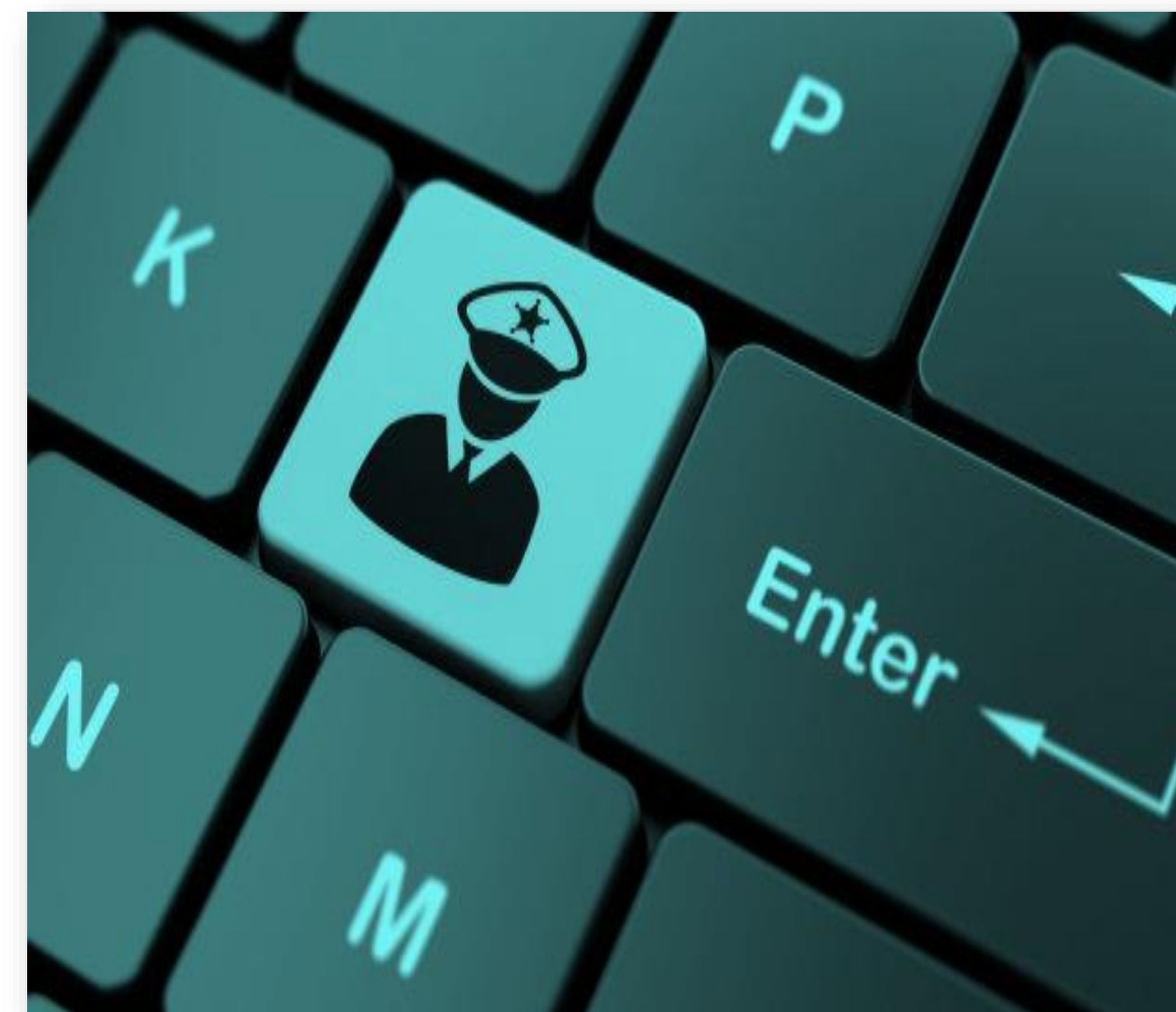
Оцінка ризиків
Тренінги
Політики і процедури
Технічний захист даних

DPO (Data Protection
Officer)
Аудит
Моніторинг

Хто такий «Data Protection Officer» та у яких випадках його необхідно призначати?

Data Protection Officer (DPO) - це особа, яка повинна призначатися контролером та/або оператором даних з метою забезпечення відповідності їхньої діяльності положенням GDPR у наступних випадках:

- ① опрацювання здійснює публічний орган або установа, за винятком судів, що діють як судові інстанції;
- ② основні види діяльності контролера або оператора становлять операції опрацювання, які, в силу їхньої специфіки, обсягів та/чи цілей, **вимагають регулярного, систематичного і широкомасштабного моніторингу суб'єктів даних;** або
- ③ основні види діяльності контролера або оператора становлять широкомасштабне опрацювання спеціальних категорій даних та персональних даних про судимості і кримінальні злочини.



Коло обов'язків Data Protection Officer

- ① інформувати та надавати рекомендації контролеру або оператору і працівникам, які здійснюють опрацювання, щодо їхніх обов'язків відповідно до цього Регламенту та інших положень про захист даних ЄС чи держави-члена.
- ② здійснювати моніторинг відповідності цього Регламенту іншим положенням про захист даних ЄС або держави-члена та політиці контролера або оператора щодо захисту персональних даних, у тому числі, розподілу обов'язків, підвищення обізнаності та підготовки персоналу, залученого до операцій опрацювання, та відповідних перевірок;
- ③ на запит, надавати рекомендації щодо оцінювання впливу на захист даних і здійснювати моніторинг його проведення;
- ④ діяти як координаційний центр для наглядового органу з питань, що стосуються опрацювання, в тому числі, попередньої консультації, і надавати консультації за необхідності, щодо будь-якого іншого питання.



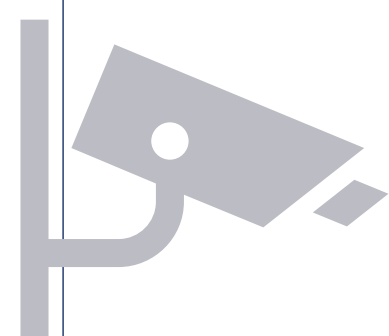
GDPR Compliance checklist



Аналіз даних



Дотримання прав



Керування
даними



Публічна
документація



Безпека даних

ДЯКУЮ ЗА УВАГУ!



Київ, вул. Дегтярна, 8



(044) 337 70 07



info@esquires.ua



<http://esquires.ua>

