Тетяна Андріанова, генеральний директор компанії Nota Group, голова комітету корпоративної безпеки групи компаній «Октава», член правління Асоціації професіоналів корпоративної безпеки

Шлях до безпеки даних: крок перший – DPIA

Новий регламент Євросоюзу щодо захисту персональних даних, який вступив у силу в кінці травня, приносить українському бізнесу більше питань, ніж відповідей. І якщо з абревіатурою GDPR керівники компаній вже звиклись, про співробітника з посадою DPO хоча б чули, то справжній жах вселяє ще одне нове слово з європейського регламенту – DPIA. Що це й чим загрожує? Чи такий страшний вовк, як їм лякають? Зараз будемо розбиратися і з'ясуємо кілька найголовніших питань.

Давайте згадаємо ази. З кінця травня український бізнес активно обговорює новий регламент щодо захисту даних, який набув чинності в ЄС, – General Data Protection Regulation (https://eur-lex.europa.eu/eli/reg/2016/679/oj). Дане положення поширюється не тільки на резидентів Євросоюзу, але й на компанії з третіх країн, які обробляють персональні дані європейських громадян. Відповідно, під удар потрапляють і українські фірми, які пропонують товари й послуги громадянам і резидентам ЄС. Це можуть

бути готелі, клініки, інтернет-магазини, служби поштових пересилань, банки, IT-компанії тощо. Також нові правила можуть торкнутися дослідних організацій, які через інтернет моніторять поведінку європейців. Змусити український бізнес впровадити стандарти GDPR ЄС поки не може, але в разі великої витоку даних штраф за недотримання правил може досягати 20 млн $, або 4% від загального річного обороту.

Що таке DPIA?

Ця, на перший погляд грізна, абревіатура розшифровується як Data Protection Impact Assessment, що в перекладі означає «оцінка впливу на захист даних». Якщо говорити конкретніше, то відповідно до частини 1 статті 35 Регламенту і (89)–(96) декларативної частини Регламенту ця процедура повинна допомогти виявити високі ризики, які можуть виникнути в процесі обробки персональних даних громадян Євросоюзу, і повинна бути ініційована до початку їх обробки. Логічно, що, якщо обробка почалася до набрання чинності GDPR, оцінку ризиків рекомендується ініціювати якомога раніше в поточному відрізку часу. Тобто, згідно з регламентом, це один із організаційних заходів, який необхідно провести на підприємстві, щоб впровадити стандарти GDPR.

У яких випадках потрібно проводити DPIA?

Виходячи зі своєї практики, моя порада: в будь-яких, якщо ви маєте справу зі збором і обробкою персональних даних європейців. Адже в бізнесі не буває зайвих запобіжних заходів, тут вже вам приймати рішення, чи ризикувати діловою репутацією та своїм дітищем у цілому. Але все ж є ряд ситуацій, коли DPIA необхідна як повітря. Відповідно до частини 3 статті 35 Регламенту DPIA необхідна:

• якщо тип обробки з використанням нових технологій може призвести до виникнення високого ризику порушень прав і свобод фізичних осіб;

• якщо систематично за допомогою автоматизованої обробки оцінюються великі масиви даних;

• якщо обробляються «чутливі дані» (про здоров'я, релігію, політичні погляди, біометричні дані) або персональні дані про судимості й кримінальні злочини.

Хто, коли й як повинен проводити DPIA?

Своїм клієнтам я раджу проводити оцінку до початку обробки персональних даних, тобто ще до запуску продукту. Якщо впровадження GDPR відбувається вже на етапі повноцінно функціонуючого продукту, то DPIA потрібно провести якомога швидше. Після цього процедуру варто повторювати при впровадженні нових технологій або організаційних заходів. Наприклад, якщо ви поміняли програмне забезпечення або спосіб зберігання даних. Складання рекомендацій щодо оцінки впливу на захист даних – один із невід'ємних обов'язків DPO (ч. 2 ст. 35 Регламенту). Згідно з регламентом, звіт повинен включати повний опис операцій по обробці даних і їх цілей, оцінку необхідності проведення кожного виду обробки, виходячи з принципу мінімізації даних, оцінку всіх можливих ризиків для європейських громадян, список заходів для подолання ризиків.

Навіщо це потрібно?

Найпростіша відповідь: це допоможе впровадити й дотримуватися стандартів GDPR. А відповідно, допоможе адекватно оцінити ризики й мінімізувати їх «за секунду до». А це, у свою чергу, вбереже ваш бізнес від багатомільйонних штрафів у разі витоку особистих даних користувачів. А якщо це станеться, у суді факт проведення компанією DPIA може стати вагомим аргументом на користь підприємства. Ну й ще один з менш очевидних плюсів: проведення перевірки додасть «зірочку» на погони вашої ділової репутації. Для європейських партнерів це буде вирішальним фактором співпраці, а для українців – авансом довіри до компанії, яка дотримується європейських стандартів захисту персональних даних.

Підсумувати все вищесказане хочу улюбленим прислів'ям юристів: «Попереджений – значить озброєний». Витрачати свої гроші, час і ресурси на необов'язкову, на перший погляд, оцінку DPIA? Однозначно так! Навіщо? Тому що тільки таким шляхом ваш бізнес може планомірно й правильно впровадити європейський регламент GDPR. А це, у свою чергу, може допомогти вам завоювати європейські ринки й зберегти кругленьку суму в разі форс-мажору. Так що моя порада: довірте це питання сертифікованому DPO (офіцеру із захисту даних) і будьте впевнені в завтрашньому дні!