Некіт Катерина Георгіївна

Національний університет «Одеська юридична академія»,

доцент кафедри цивільного права, кандидат юридичних наук, доцент

ЗНАЧЕННЯ GDPR (GENERAL DATA PROTECTION REGULATION) ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

Одним з найважливіших проблемних питань у сфері Інтернету речей на сьогодні є питання захисту персональних даних.

З метою забезпечення захисту персональних даних у Європейському Союзі було розроблено нові правила обробки персональних даних та прийнято Загальний регламент із захисту даних (Регламент ЄС 2016/679 від 27 квітня 2016 р. або GDPR — General Data Protection Regulation), який набуває чинності з травня 2018 року, після чого компанії, що порушують правила щодо обробки персональних даних ризикують бути притягнутими до відповідальності із накладенням штрафів до 20 мільйонів євро або 4% річного доходу компанії. Основні принципи обробки персональних даних за GDPR такі:

1) законність, справедливість і прозорість: персональні дані повинні оброблятися законно, справедливо і прозоро. Будь-яку інформацію про цілі, методи і обсяги обробки персональних даних слід висловлювати максимально доступно і просто;

2) обмеження мети: дані повинні збиратися і використовуватися виключно в тих цілях, які заявлені компанією (онлайн-сервісом);

3) мінімізація даних: не можна збирати особисті дані в більшому обсязі, ніж це необхідно для цілей обробки;

4) точність: особисті дані, які є неточними, повинні бути видалені або виправлені (на вимогу користувача);

5) обмеження зберігання: особисті дані повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єкти даних на строк не більш, ніж це необхідно для цілей обробки;

6) цілісність і конфіденційність: при обробці даних користувачів компанії зобов'язані забезпечити захист персональних даних від несанкціонованої або незаконної обробки, знищення і пошкодження [1].

Однією з важливих для належного розвитку IoT новацій, закріплених у GDPR, є так звані дружні для інновацій правила, відповідно до яких гарантії захисту даних у продуктах та послугах, що розробляються, повинні бути забезпечені на самих ранніх стадіях розвитку, тобто ще на стадії проектування. Це правило має назву Privacy by Design або Data Protection by Design. Основними принципами Privacy by Design є такі:

1) превентивні заходи, а не тільки усунення наслідків: вбудовування конфіденційності в конструкцію системи повинне бути активним, а не обмежуватися лише заходами по усуненню наслідків. Такий підхід передбачає і запобігає випадкам порушення конфіденційності ще до того, як вони відбуваються. Іншими словами, особиста інформація повинна бути захищена до того, як система запущена в роботу, а не після виявлення порушень конфіденційності;

2) конфіденційність як стандартна установка: Privacy by Design прагне досягти максимального ступеня захисту особистої інформації, гарантуючи, що персональні дані захищені автоматично в тій або іншій інформаційній системі або ділових відносинах. Навіть якщо індивідуум не вживає ніяких заходів, його особиста інформація залишається надійно захищеною. Не вимагається ніяких дій з боку індивідуума для захисту особистої інформації, – система вже спочатку містить в собі необхідні установки;

3) конфіденційність як частина структури: захист особистої інформації повинен стати невід'ємною частиною архітектури будь-якої інформаційної

системи або ділових відносин. Це не якийсь додатковий компонент, внесений в систему пост-фактум;

4) повна функціональність із сумарним позитивним результатом: Privacy by Design не шукає приводів для помилкової дихотомії, таких, наприклад, як зміцнення безпеки системи на противагу захисту особистої інформації, демонструючи, що можна забезпечити і те, і інше;

5) захист особистої інформації впродовж всього циклу її збору, зберігання, обробки і знищення: конфіденційність повинна бути вбудована в систему ще до початку збору даних. Більш того, цей захист повинен надійно розповсюджуватися на весь цикл зберігання і обробки даних; іншими словами, збереження даних має важливе значення для конфіденційності від моменту запуску системи і до кінця її існування. Це гарантує надійне зберігання даних, а після закінчення їх використовування – надійне і своєчасне знищення;

6) доступність і відвертість: всі компоненти і операції залишаються відкритими і доступними, як для користувачів, так і для тих, хто забезпечує даний вид сервісу;

7) дотримання конфіденційності користувачів: система повинна бути орієнтована на користувача. Це досягається такими заходами, як захист особистої інформації за умовчанням, своєчасне повідомлення про збір особистої інформації, надання користувачу свободи вибору в зручній і зрозумілій формі [2].

Крім того, що наведені положення щодо захисту персональних даних варті уваги українського законодавця з метою забезпечення захисту персональних даних українських громадян шляхом прийняття аналогічного акту, необхідно пам’ятати, що Регламент ЄС 2016/679 носить екстериторіальний характер, тобто застосовується до усіх компаній, що обробляють персональні дані громадян та резидентів ЄС, незалежно від місця знаходження такої компанії.

Список використаної літератури:

1. GDPR – новые правила обработки персональных данных в Европе для международного IT-рынка. URL: https://habrahabr.ru/company/digitalrightscenter/blog/344064/

2. Кавукиан Э. Privacy by Design: 7 основополагающих принципов. URL: https://online.zakon.kz/Document/?doc_id=31633216#pos=0;0