УДК 004.056

Д. В. Дерун

GDPR: ОСНОВНІ ПОЛОЖЕННЯ ТА ВИКОРИСТАННЯ В СУЧАСНОМУ СВІТІ

[1] Вінницький національний технічний університет;

Анотація

Досліджено особливості регламенту Європейського Союзу GDPR (General Data Protection Regulation), його основні положення та умови використання.

Ключові слова: GDPR, персональні дані, чутливі дані, політика захисту персональних даних, захист персональних даних.

Abstract

The features of the European Union's GDPR (General Data Protection Regulation) have been studied, along with its main provisions and conditions of use.

Keywords: GDPR, personal data, sensitive data, protection policy, personal data protection.

Вступ

Сучасний світ наповнений інтернетом та електронними ресурсами. Через інтернет зараз здійснюється обробка даних для різних завдань. Проте ризики сучасного світу також потребують відповідного захисту персональних даних користувачів, для цього були створені різноманітні політики та регламенти, один з яких GDPR [1].

GDPR (General Data Protection Regulation) – це регламент Європейського Союзу, який набув чинності 25 травня 2018 року. Він встановлює загальні правила захисту персональних даних громадян ЄС [2].

Метою роботи є дослідження регламену GDPR, його положень, особливостей та санкцій за порушення. А також можливості його використання для сучасного бізнесу та відмінності для різних типів онлайн-платформ.

Результати дослідження

До основних положень регламенту GDPR можна віднести [3].

1) Законність, справедливість та прозорість – це означає, що організації мають інформувати користувачів про мету, час зберігання та можливих одержувачів даних.

2) Обмеження цілей – дані зберігаються для чітких цілей і не можуть бути використані якось інакше без згоди користувача.

3) Мінімізація даних – організація зобов’язана збирати лише необхідні дані для досягнення цілі.

4) Точність даних – постійна актуалізація та оновлення даних.

5) Обмеження строку зберігання – після досягнення цілі дані обов’язково видаляються.

6) Цілісність і конфіденційність – організація зобов’язана забезпечити повний захист даних користувача.

7) Підзвітність – організація зобов’язана документувати кожний крок обробки даних користувача.

8) Згода на обробку даних – згода має бути максимально конкретизованою, окрім того користувачі мають можливість в будь який момент розірвати згоду чи внести свої корективи.

9) Права суб’єктів даних – суб’єкти мають постійне право на доступ, виправлення і також видалення даних.

10) Повідомлення про порушення даних – якщо стався витік даних, організація зобов’язана про це повідомити відповідні органи не довше ніж за 72 години.

11) Офіцер із захисту даних – DPO (Data Protection Officer) несе відповідальність за дотримання компанією чи організацією усіх вимог GDPR.

Враховуючи, що весь світ співпрацює з країнами Європейського Союзу – GDPR стає все більш ак-

туальним. Станом на сьогодні його активно використовує бізнес, що обробляє дані громадян країн ЄС, будь-які сайти, сервіси, онлайн-магазини, що працюють з ЄС також мають відповідати стандартам GDPR, це також стосується і фінансових установ, тобто банків, фінансових сервісів, страхових компаній і звичайно ж, медичні установи також мають строго дотримуватись положень GDPR.

Варто зазначити, що для кожного типу сервісу положення регламенту GDPR будуть дещо відрізнятись, враховуючи мету збирання даних. Так наприклад, для медичних установ політика GDPR буде більш строга, окрім того, організація не має жодного права обробляти чутливі дані без згоди клієнта. Для сайтів соціальних мереж обов'язковою умовою буде – захист конфіденційності профілів, згода на обробку даних та право на видалення даних [4].

Як і для кожної політики, для GDPR Європейський Союз також ввів різноманітні види покарань за недотримання положень регламенту. Ці покарання можуть відрізнятись залежно від масштабу порушення та наслідків, але ось кілька найбільш вживаних [5]:

1) фінансові штрафи – штраф за порушення політики може сягати 20 мільйонів євро або 4% світового річного обороту компанії – залежить від того, яка сума більше;

2) цивільна відповідальність – фізичні особи мають право на компенсацію за збитки, які спричинило порушення GDPR. Варто зазначити, що збитки можуть бути як матеріальні, так і моральні;

3) адміністративні санкції – при виявлені порушень, спеціальні органи нагляду можуть видавати попередження, а також вимагати виправлення, обмеження або й взагалі видалення даних;

4) кримінальна відповідальність – у деяких країнах ЄС за порушення GDPR можуть накладати кримінальні санкції, особливо якщо мова йде про серйозні порушення з важкими наслідками;

5) заборона на обробку даних – спеціальні органи нагляду можуть тимчасово або назавжди заборонити організаціям обробляти персональні дані користувачів.

Висновки

Отже, регламент Європейського Союзу GDPR має все ширше і ширше використання по всьому світу. Основні положення регламенту є досить строгими, що забезпечує максимальний захист персональних даних користувачів. За порушення, недотримання регламенту на компанію чекає так зване покарання, яке може бути у вигляді як фінансового штрафу, так і навіть кримінального провадження та заборону на обробку даних користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. IEEE Xplore. Challenges and Enablers for GDPR Compliance: URL: https://ieeexplore.ieee.org/abstract/document/10540423 (дата звернення 11.03.2025)
2. Science Direct. An insightful survey from the GDPR perspective: URL: https://www.sciencedirect.com/science/article/pii/S0167404821002261 (дата звернення 11.03.2025)
3. Intersoft Consulting. General Data Protection Regulation: URL: https://gdpr-info.eu/ (дата звернення 11.03.2025)
4. European Union. Document 32016R0679: URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (дата звернення 11.03.2025)
5. Legal IT Group. GDPR. Тренди 2019: URL: https://legalitgroup.com/vebinar-zahist-personalnih-danih-gdpr-trendi-2019/ (дата звернення 11.03.2025)

Дерун Дарина Вадимівна – студентка групи 1БС-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: dashaderun04@gmail.com.

Науковий керівник: ***Войтович Олеся Петрівна*** – доцент кафедри Захисту інформації, Вінницький національний технічний університет, м. Вінниця

Derun Daryna V. – Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: dashaderun04@gmail.com.

Supervisor: ***Voitovych Olesya P.*** – Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia