УДК: 004.056.5:342.7

Печериця Д. В., здобувач вищої освіти,
Чернов Д. В., канд. техн. наук,
доцент кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

ЄВРОПЕЙСЬКИЙ РЕГЛАМЕНТ З ОХОРОНИ ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. У сучасному цифровому світі обробка персональних даних стала невід'ємною частиною функціонування бізнесу та державних інституцій. Загальний регламент про захист даних (GDPR), запроваджений Європейським Союзом, встановив новий глобальний стандарт у цій сфері. У цій роботі представлено аналіз ключових положень GDPR, включно з його основними принципами, правами суб'єктів даних та обов'язками контролерів і обробників. Також розглянуто екстериторіальну сферу дії регламенту та механізми відповідальності за його порушення, що мають значний вплив на організації по всьому світу.

Ключові слова: GDPR, Загальний регламент про захист даних, персональні дані, захист даних, суб'єкт даних, контролер даних, обробник даних, права суб'єктів даних.

Актуальність теми дослідження. Актуальність полягає у необхідності адаптації глобальних бізнес-процесів до жорстких вимог захисту приватності, встановлених GDPR.

Зі стрімким зростанням обсягів даних, що збираються та обробляються (Big Data, AI, IoT), зростає і занепокоєння громадян щодо їх конфіденційності. GDPR став першим комплексним та екстериторіальним законом, що надає суб'єктам даних реальні важелі контролю та запроваджує безпрецедентно високі штрафи за порушення [1].

Багато організацій за межами ЄС, включно з українськими компаніями, що працюють на європейський ринок або навіть просто мають відвідувачів сайта з ЄС, зіткнулися з необхідністю кардинального перегляду своїх політик роботи з даними. На відміну від попередніх директив, GDPR вимагає не просто формального дотримання, а впровадження проактивних підходів, як-от «конфіденційність за задумом» (Privacy by Design) та «конфіденційність за замовчуванням» (Privacy by Default). Нерозуміння або ігнорування цих вимог призводить до значних фінансових та репутаційних ризиків.

Основна частина. Загальний регламент про захист даних (GDPR) [1] – це фундаментальний правовий акт ЄС, що набув чинності 25 травня 2018 р. Його головна мета – гармонізувати законодавство про захист даних у всіх країнах ЄС та посилити права громадян на контроль над своїми персональними даними.

Регламент має екстериторіальну дію. Він застосовується до всіх компаній, що обробляють персональні дані резидентів ЄС, незалежно від місцезнаходження самої компанії.

Це стосується випадків, коли компанія:

– має представництво в ЄС;

– пропонує товари чи послуги громадянам в ЄС (навіть безкоштовно);

– здійснює моніторинг поведінки громадян в ЄС (наприклад, через cookie-файли або профілювання).

Основні принципи обробки даних GDPR базується на семи ключових принципах (Стаття 5), яких контролери даних зобов'язані дотримуватися [2]:

– законність, справедливість і прозорість – обробка має мати законну підставу, бути чесною та зрозумілою для суб'єкта;

– обмеження мети – дані збираються для чітких, законних цілей і не обробляються у спосіб, несумісний з цими цілями;

– мінімізація даних – обсяг даних має бути адекватним, релевантним і обмеженим лише тим, що необхідно для визначеної мети;

– точність – дані мають бути точними та оновлюватися в разі потреби;

– обмеження зберігання – дані зберігаються у формі, що дозволяє ідентифікацію, не довше, ніж це необхідно;

– цілісність і конфіденційність – забезпечення належної безпеки даних (захист від несанкціонованої обробки, втрати, знищення);

– підзвітність – контролер несе відповідальність за дотримання всіх принципів і повинен бути в змозі це продемонструвати.

Права суб'єктів даних GDPR значно розширив права фізичних осіб (суб'єктів даних), надавши їм:

– право на доступ (Стаття 15) – можливість отримати копію своїх даних та інформацію про те, як вони обробляються;

– право на виправлення (Стаття 16) – вимагати виправлення неточних даних;

– право на забуття (Стаття 17) – вимагати видалення своїх даних за певних умов (наприклад, дані більше не потрібні, відкликано згоду);

– право на обмеження обробки (Стаття 18) – «заморозити» обробку даних у спірних ситуаціях;

– право на переносимість даних (Стаття 20) – отримати свої дані у структурованому, машиночитаному форматі та передати їх іншому контролеру;

– право на заперечення (Стаття 21) – заперечувати проти обробки даних, зокрема проти прямого маркетингу.

Обов'язки та відповідальність. Регламент покладає чіткі обов'язки на контролерів (тих, хто визначає мету обробки) та обробників (тих, хто обробляє дані за дорученням).

Ключові обов'язки:

– отримання чіткої згоди. Згода має бути вільною, конкретною, інформованою та однозначною. Мовчання або попередньо проставлені «галочки» не є згодою [3];

– призначення Data Protection Officer (DPO). Обов'язкове для держорганів та компаній, що проводять масштабний моніторинг або обробку чутливих даних;

– проведення Оцінки впливу на захист даних (DPIA). Обов'язкова для ризикованих видів обробки (Стаття 35);

– повідомлення про витік даних. Обов'язок повідомити наглядовий орган протягом 72 годин після виявлення витоку (Стаття 33).

За порушення GDPR передбачено два рівні адміністративних штрафів:

– до €10 млн або 2 % від загальносвітового річного обороту (за менш значні порушення, наприклад, щодо обов'язків контролера).

– до €20 млн або 4 % від загальносвітового річного обороту (за серйозні порушення, наприклад, принципів обробки або прав суб'єктів) [1; 4].

Результати та перспективи розвитку. За роки після впровадження GDPR став де-факто «золотим стандартом» для законодавства про приватність у всьому світі, вплинувши на розробку аналогічних законів в інших юрисдикціях (наприклад, CCPA в Каліфорнії, LGPD в Бразилії). Компанії були змушені впровадити більш прозорі політики конфіденційності та надати користувачам реальний контроль над їхньою інформацією. Подальший розвиток пов'язаний із вирішенням складних питань застосування GDPR до новітніх технологій, як-от штучний інтелект, машинне навчання та блокчейн, де принципи мінімізації даних чи «права на забуття» стикаються з технічними обмеженнями. Очікується подальше посилення наглядової практики та збільшення кількості транскордонних розслідувань.

Список використаних джерел

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 02.11.2025).

2. Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, 2017. 452 p.

3. European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679. URL: https://surl.lu/vfuvsw (дата звернення: 03.11.2025).

4. Bygrave L. A. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 2020. 800 p.