importance of both international and domestic legal frameworks in addressing serious crimes.

Bibliography:

1. Shabas, W. A. An Introduction to the International Criminal Court. 6th edition. Cambridge : Cambridge University Press, 2020. 412 p.

2. Bassiouni, M. Cherif. International Crimes: Ratione Materiae of International Criminal Law // In: Bassiouni, M. Cherif (ed.). *International Criminal Law*. 3rd edn. Vol. I. Leiden : Brill, 2008. P. 129–135.

3. Fabri, H. R. International Courts and Tribunals: The Performance of International Courts and Tribunals. Leiden : Brill, 2019. 305 p.

4. McDermott, Y. *Fairness in International Criminal Trials.* Oxford : Oxford University Press, 2016. 250 p.

5. Gaeta, P. (ed.). The UN Genocide Convention: A Commentary. Oxford : Oxford University Press, 2009. 450 p.

6. Stahn, C. (ed.). The Law and Practice of the International Criminal Court. Oxford : Oxford University Press, 2015. 680 p

DOI https://doi.org/10.36059/978-966-397-479-8-31

КЛЮЧОВІ ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ЗГІДНО З ЗАГАЛЬНИМ РЕГЛАМЕНТОМ ПРО ЗАХИСТ ДАНИХ (GDPR) ТА ПЕРСПЕКТИВИ ЇХ ІМПЛЕМЕНТАЦІЇ

Старчук Є. В.
аспірант
ПВНЗ «Європейський університет»
Науковий керівник: ***Тимошенко О. А.***
кандидат юридичних наук,
доцент кафедри права
ПВНЗ «Європейський університет»
м. Київ, Україна

Інтеграція України до ЄС є на сьогодні одним з двох ключових напрямків, на яких будує своє майбутнє наша країна. Цей напрямок передбачає послідовне та безперервне інтегрування норм ЄС в правове поле України. Відповідно до ст. 15 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами [1], сторони

домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia, обмін інформацією та експертами.

Згідно з повідомленням Кабінету Міністрів України [2] Україна мала вже цього року схвалити Національну програму адаптації законодавства України до права Європейського Союзу. Однак, як ми бачимо її на сьогодні не схвалено, тому це питання залишається наразі одним з пріоритетних.

Так, одним з найважливіших питань є максимальна гармонізації національного законодавства з Загальним регламент про захист даних (GDPR) [3], що дозволяє максимально адаптувати український бізнес до вимог цього документа.

На сьогодні, діюча редакція закону України «Про захист персональних даних» [4] не повністю відповідає основним принципам GDPR, тому необхідно детально проаналізувати ці принципи та розробити відповідні методи їх імплементації.

Згідно із Загальним регламентом про захист даних (GDPR), принципи та норми захисту фізичних осіб під час обробки їхніх персональних даних гарантують дотримання фундаментальних прав і свобод незалежно від громадянства або місця проживання. Особливий акцент зроблено на праві на захист персональних даних. Детальний виклад принципів обробки закріплений у Розділі II GDPR, який є основним джерелом регулювання цих аспектів.

Принцип законності

Цей принцип наголошує, що обробка персональних даних можлива лише за наявності правових підстав. Відповідно до статті 6 GDPR, дані можуть бути оброблені лише у випадках:

– надання згоди суб'єктом даних;
– виконання умов договору;
– виконання юридичних зобов’язань;
– захисту життєво важливих інтересів суб'єкта;
– реалізації завдань у суспільних інтересах або здійснення офіційних повноважень;
– для законних інтересів контролера даних, якщо вони не порушують права суб'єкта даних.

Дотримання цього принципу є основою для захисту прав осіб і збереження довіри до обробки персональних даних.

Принцип правомірності

Цей принцип вимагає, щоб обробка персональних даних здійснювалася чесно і законно. Це означає, що заборонено використовувати шахрайські або обманні методи, а також обробляти дані у спосіб, який не відповідає очікуванням суб'єкта даних. Дотримання принципу правомірності є важливим для запобігання потенційним зловживанням і несправедливому використанню інформації суб'єктів даних, захищаючи їхні права.

Принцип прозорості

Прозорість обробки даних передбачає інформування суб'єктів даних про всі аспекти обробки їхньої інформації. Це включає чітке повідомлення про те:

- які дані збираються;
- як і для яких цілей вони використовуються;
- з ким вони можуть бути поділені;
- які заходи захисту застосовуються.

Прозорість сприяє підвищенню довіри користувачів до систем обробки даних і забезпечує відповідальність контролерів.

Принципи законності, правомірності та прозорості є основою етичної та ефективної системи захисту персональних даних. Вони гарантують, що права суб'єктів даних захищаються на найвищому рівні, а обробка інформації відповідає встановленим правовим стандартам.

Принцип цільового обмеження

Принцип цільового обмеження передбачає, що персональні дані повинні збиратися виключно для конкретних, чітко визначених і законних цілей. Використання зібраних даних для інших, несумісних із початковими, цілей забороняється. Якщо виникає потреба у новій меті обробки, така обробка повинна:

- бути дозволена законодавством;
- супроводжуватися отриманням додаткової згоди суб’єкта даних.

Цей принцип має важливе значення для забезпечення відповідального використання персональних даних і зменшення ризиків їх неналежного оброблення.

ЄСПЛ неодноразово підтверджував важливість цільового обмеження. У справі S. and Marper v. the United Kingdom [5], Суд визнав, що зберігання біометричних даних осіб, які не були засуджені, без чіткої мети є порушенням права на приватність, гарантованого статтею 8 Європейської конвенції з прав людини. Суд зазначив, що подальша обробка даних без узгоджених цілей створює загрозу для приватності та демократичних стандартів.

Дотримання принципу цільового обмеження сприяє захисту фундаментальних прав осіб і забезпечує, щоб дані використовувалися тільки

в рамках узгоджених правових меж. Це підвищує рівень довіри до систем обробки даних і зменшує ризики їх неналежного використання.

Принцип мінімізації даних

Принцип мінімізації даних встановлює, що організації повинні збирати лише ті персональні дані, які є адекватними, релевантними та обмеженими до мінімуму, необхідного для досягнення чітко визначених цілей. Це означає, що дані, які не мають прямого відношення до поставлених завдань, не повинні оброблятися.

Принцип допомагає мінімізувати ризики, пов'язані з витоками або неправомірним використанням даних та зменшує вплив обробки на приватність осіб.

Організації, які дотримуються цього принципу, можуть ефективніше контролювати дані та гарантувати їх захист.

Німецький досвід: Німецьке Федеральне управління з інформаційної безпеки (BSI) також виділяє мінімізацію даних як важливий аспект безпеки, особливо в державному секторі. У своїх щорічних звітах [6] про IT-безпеку BSI наголошує на необхідності зменшення обсягів обробки даних для захисту конфіденційності.

Принцип мінімізації даних є ключовим для забезпечення ефективної та відповідальної обробки інформації. Його дотримання не лише відповідає вимогам законодавства, але й дозволяє організаціям краще захищати дані, мінімізувати ризики та підвищувати довіру користувачів.

Принцип точності

Принцип точності встановлює, що персональні дані мають бути актуальними, коректними та оновлюватися за необхідності. Згідно зі Статтею 5(1)(d) GDPR, дані, які є неточними з урахуванням цілей обробки, повинні бути виправлені або видалені без затримок. Це вимагає від контролерів даних впровадження ефективних процедур для постійного перегляду, коригування та оновлення даних.

Контролери повинні забезпечити:

– Можливість суб'єктам даних коригувати свої дані у разі помилок.

– Регулярний перегляд баз даних для усунення неточностей або застарілої інформації.

– Використання технологій для автоматичного виявлення некоректних даних.

Приклади реалізації:

Фінансовий сектор. У банківській сфері точність даних клієнтів є критичною для фінансових операцій. Наприклад, некоректна адреса чи контактна інформація може призвести до помилкових транзакцій або втрати зв'язку з клієнтом. Для запобігання цьому банки регулярно перевіряють і оновлюють дані клієнтів через CRM-системи та процеси повторної верифікації.

Охорона здоров'я. У медичній сфері точність даних безпосередньо впливає на життя пацієнтів. Неточна інформація про діагнози, алергії чи ліки може призвести до помилкових рішень щодо лікування. Лікарні використовують електронні медичні записи (EMR) з регулярними оновленнями, щоб зменшити ризик помилок і забезпечити безпечне лікування пацієнтів.

Принцип точності є основоположним для забезпечення якості обробки даних. Дотримання цього принципу дозволяє знизити ризики, пов'язані з використанням неправдивої чи застарілої інформації, а також підвищує довіру до процесів обробки даних.

Принцип обмеження зберігання

Принцип обмеження зберігання, визначений у статті 5(1)(e) GDPR, встановлює, що персональні дані повинні зберігатися лише протягом часу, необхідного для досягнення цілей їх обробки. Після завершення цих цілей дані мають бути видалені або анонімізовані, щоб виключити можливість ідентифікації суб'єкта даних.

Основні аспекти принципу:

1. Обмеження часу зберігання:

– Організації зобов'язані визначати строки зберігання даних на етапі їх збору.

– Дані повинні бути видалені або анонімізовані після досягнення поставлених цілей.

2. Запобігання ризикам:

– Принцип зменшує ризик витоку даних, несанкціонованого доступу чи неправомірного використання.

– Накопичення непотрібних даних створює ризик додаткових витрат і загроз безпеці.

Приклад із практики ЄСПЛ:

У справі Gaughran v. the United Kingdom (2020) [7] Європейський суд з прав людини ухвалив, що тривале зберігання поліцейських записів, таких як відбитки пальців, ДНК та фотографії засудженого, порушувало право на приватне життя. Суд зазначив, що зберігання даних без належного перегляду чи обмеження строків є непропорційним і становить загрозу для приватності. Це рішення демонструє, що організації повинні періодично перевіряти необхідність зберігання даних і впроваджувати чіткі політики видалення даних після їх використання.

Принцип цілісності та конфіденційності

Цей принцип гарантує, що персональні дані повинні бути захищені від:

– Несанкціонованого доступу.

– Знищення або втрати.

– Неправомірної обробки.

– Дані повинні залишатися точними та повними під час зберігання, передачі та обробки. Використання систем контролю змін допомагає уникнути втрати чи пошкодження даних.

– Доступ до даних дозволений тільки уповноваженим особам або системам.

– Для захисту даних використовуються сучасні технології, як-от шифрування, токенізація, захищені канали передачі.

У банківських установах застосовується багаторівневий захист для забезпечення конфіденційності та цілісності даних клієнтів.

У сфері охорони здоров'я використовуються захищені медичні бази даних, які обмежують доступ лише до персоналу, що має на це дозвіл.

Принципи обмеження зберігання, цілісності та конфіденційності сприяють зменшенню ризиків, забезпеченню прав суб'єктів даних і побудові довіри до обробки інформації. Їх впровадження є обов'язковим для дотримання норм GDPR і підвищення загальної ефективності систем управління даними.

Саме з використанням вищевказаних принципів і має здійснюватися реалізація Національної програми адаптації законодавства України до права Європейського Союзу в частині захисту персональних даних. Важливим кроком на цьому шляху було створення проєкту Association4U, який підтримує формування та посилення спроможності публічної адміністрації в Україні щодо розроблення [8] та реалізації ключових реформ, обумовлених Угодою про асоціацію та Договором про поглиблену та всеохоплюючу зону вільної торгівлі між Україною та ЄС, здійснюючи це через сприяння наближенню українського законодавства до законодавства ЄС та підтримку комунікації Уряду з питань європейської інтеграції.

Література:

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014.

2. Прем’єр-міністр: Цього року Уряд схвалить Національну програму адаптації законодавства України до права Європейського Союзу. URL: https://www.kmu.gov.ua/news/premier-ministr-tsoho-roku-uriad-skhvalyt-natsionalnu-prohramu-adaptatsii-zakonodavstva-ukrainy-do-prava-ievropeiskoho-soiuzu

3. Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб у зв’язку з обробкою персональних даних та про вільний рух таких даних. *Офіційний журнал Європейського Союзу*. 2016. L 119. С. 1–88.

4. Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України (ВВР)*. 2010. № 34, ст. 481).

5. Справа "S. і Марпер проти Сполученого Королівства" (S. and Marper v. the United Kingdom), заяви № 30562/04 і 30566/04, рішення ЄСПЛ від 4 грудня 2008 р. URL: https://hudoc.echr.coe.int/eng?i=001-90051

6. ENISA Annual Activity Report 2022. Європейське агентство з кібербезпеки (ENISA). 2022. URL: https://www.enisa.europa.eu/publications/corporate-documents/enisa-annual-activity-report-2022.pdf/view (дата звернення: 10.10.2023).

7. Справа "Гофран проти Сполученого Королівства" (Gaughran v. the United Kingdom), заява № 45245/15, рішення ЄСПЛ від 13 лютого 2020 р. URL: https://hudoc.echr.coe.int/eng?i=001-200817

8. Огляд розробок у законодавстві ЄС, правовому аналізі та адаптації законодавства ЄС в Україні. Association4U. URL: https://eu-ua.kmu.gov.ua/sites/default/files/inline/files/eu_law_and_legal_approximation_review_for_ukraine_-_a4u_ii_newsletter_no_56.docx (дата звернення 07.11.2022).

DOI https://doi.org/10.36059/978-966-397-479-8-32

МОЖЛИВІСТЬ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЕЛЕКТРОННІ МАЙДАНЧИКИ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ В УКРАЇНІ

Ступак В. О.
здобувач освіти другого (магістерського) рівня
за спеціальністю 081 – Право
Державний податковий університет
Науковий керівник: ***Чайка В. В.***
доктор юридичних наук, доцент,
професор кафедри фінансового та податкового права
Державний податковий університет
м. Ірпінь, Київська область, Україна

Електронні майданчики публічних закупівель в Україні та система ProZorro є потужними інструментами для забезпечення прозорості, ефективності та відкритості використання державних коштів. Їхнє впровадження значно зменшило корупційні ризики, проте повністю їх не усунуло.