ФІНАНСОВО-КРЕДИТНА СИСТЕМА

УДК 336.71+004.78+65.001.3

Андрушків І.П.,
канд. екон. наук, доцент кафедри фінансово-економічної безпеки та банківського бізнесу,
Мушинський Б.М.*,
аспірант кафедри фінансово-економічної безпеки та банківського бізнесу,
Львівський торговельно-економічний університет

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ: НОРМАТИВНІ ВИМОГИ УКРАЇНИ ТА ЄВРОПЕЙСЬКОГО СОЮЗУ

Постановка проблеми. В умовах технологічного розвитку все гострішим постає питанням обробки, передачі та захисту персональних даних. Оскільки на сучасному етапі персональні дані використовуються всюди: і при розрахунках, і при реєстрації на сайтах, при листуванні, при отриманні банківських послуг та ін., саме тому потрібно розуміти права клієнтів та обов'язки осіб та організацій, які ці дані використовують.

Новим етапом у розвитку питань, які стосуються захисту персональних даних, стало «Загальне положення про захист персональних даних» Європейського союзу, прийняте 27 квітня 2016 року. Вимоги нового документу є неоднозначними та в дечому суперечливими, особливо зважаючи на вже існуючу законодавчу базу в кожній країні. Варто відмітити, що питання впровадження GDPR є актуальним на даний момент, тому усі дослідження та рекомендації не перевірені на практиці та можуть бути відкоректовані до 2018 року, коли документ вступить в дію.

Саме тому, виходячи з вище наведеного, ближче ознайомлення з локальними та міжнародними вимогами з питань захисту даних є надзвичайно актуальним.

Аналіз останніх досліджень і публікацій. Питання, що стосуються захисту персональних даних, досліджувались у працях таких вчених, як: Dr. Detlev Gabel, Tim Hickman, Dr. Martin Munz, Moritz Hüsch, Roland Marko, Bertrand Liard, Daren Orzechowski, Viviane Reding, Bijal Vakil, Ruth Boardman, Ariane Mole та ін.

Однак у більшості наукових досліджень недостатньо уваги приділено саме ознайомленню з локальними та міжнародними вимогами з питань захисту даних. Усе це свідчить про актуальність теми, а відтак зумовило вибір напряму дослідження в науковому і практичному аспектах.

Постановка завдання. Метою дослідження є аналіз нормативної бази, яка регулює питання захисту персональних даних, наведення основних прикладів використання законодавства на українському ринку, виділення найпріоритетніших розділів нового положення ЄС із захисту персональних даних (GDPR) та окреслення рекомендацій по впровадженню GDPR у порівнянні з існуючою Директивою із захисту персональних даних ЄС.

Виклад основного матеріалу дослідження. Для України тема персональних даних не є новинкою, проте на практиці вимоги законодавства чи світових практик використовують лише великі корпорації, які знаходяться під постійним контролем регулюючих органів. Сьогодні ми маємо один з основних законів, який регулює дане питання – Закон України «Про захист персональних даних» [8], який набув чинності 1 січня 2011 року.

Враховуючи досвід функціонування системи захисту персональних даних в Україні, 3 липня 2013 року Верховна Рада України прийняла Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [7], який набув чинності 1 січня 2014 року. Цим Законом з метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини.

Також додатковою ланкою у процесі захисту персональних даних є Закон України «Про банки і банківську діяльність» [6], а саме Глава 10 «Банківська таємниця та конфіденційність інформації».

* *Наук. керівник - Андрушків І.П., канд. екон. наук, доцент*

Цим законом накладаються додаткові обмеження по розголошенню персональних даних, які стали доступні банку у зв'язку зі здійсненням професійної діяльності та за згодою об'єктів персональних даних. Для банків також важливо виконувати вимоги материнських структур, якщо вони знаходяться в банківській групі. Часто такі вимоги є дещо жорсткішими, ніж локальні вимоги, у нашому випадку – Верховної Ради України.

У країнах Євросоюзу питаннями захисту персональних даних громадян дуже активно піклуються уже кілька років. Так, основним документом, який зобов'язував організації витримувати норми захисту та виконувати передбачені правила, була Директива Європейського Союзу з Захисту даних (95/46/ЕС), прийнята ще у далекому 1995 р. На зміну цій директиві прийшло Положення Європейського Союзу «Загальне положення про захист персональних даних» (2016/679), прийняте 27 квітня 2016 р., або скорочено – GDPR. Положення вступає в силу 25 травня 2018 року, що залишає обмаль часу для впровадження усіх його вимог [2].

GDPR містить кілька основних моментів, відмінностей від уже існуючої Директиви і тим самим робить жорсткіші умови роботи з персональними даними громадян Євросоюзу.

Першим відмінним фактором є те, що GDPR обов'язкова до виконання не лише організаціями, які є резидентами країн ЄС, але й іноземними компаніями, які використовують персональні дані громадян ЄС. Це в свою чергу спрощує вимоги через свою однорідність незалежно від територіальної приналежності компанії, але також несе в собі більші затрати на приведення роботи у відповідність до нових вимог. Влада ставить також жорстку умову у вигляді штрафу за порушення документу, рівного 20 млн. євро або 4% зведеного міжнародного доходу корпорації, в залежності від того, яка цифра буде більшою (тобто якщо фірма діє в Україні, але відноситься до групи компаній, які отримують доходи в Китаї, Індії, Європі і т.д. – штраф буде зі зведеної суми доходів по усіх ринках присутності).

Другим важливим моментом є створення Регулюючого органу у кожній країні ЄС, який буде відповідальний за імплементацію законодавства та моніторинг його виконання у своєму регіоні. Кожна компанія повинна звітуватися про виконання GDPR до відповідного регулюючого органу (Supervisory Authority), які будуть співпрацювати між собою у межах ЄС. Якщо компанія представлена у кількох країнах Євросоюзу – звітуватися необхідно до тієї SA, де представлена штаб-квартира Групи. Також буде створено Європейську раду з захисту персональних даних (EDPB), яка буде координувати роботу SAs. Винятком будуть дані, які стосуються питань національної безпеки та запобігання безробіттю – в цьому випадку дані будуть суб'єктом локальних нормативних вимог [3].

Вимоги щодо повідомлення клієнтів про їхні персональні дані залишаються і у GDPR, та є дещо розширеними. Такі повідомлення обов'язково повинні містити час обробки персональних даних та мету такої обробки. Автоматична обробка даних тепер є об'єктом для скарг, оскільки клієнти отримали змогу опротестовувати рішення прийняті щодо них, базуючись на суто технічних алгоритмах. Також важливим моментом є вимога забезпечити можливість захисту персональних даних у момент розробки бізнес-процесу або програмного комплексу. Це дає змогу компаніям розробляти рішення, які вже матимуть в собі елементи або, як мінімум, можливість для повного впровадження принципів захисту персональних даних. Також зазначається, що по замовчуванню програмні ресурси повинні бути налаштовані на найвищий ступінь захисту персональних даних (highest by default).

Новою вимогою тепер також є Аналіз впливу на захист персональних даних (Data Protection Impact Assessments) [1]. Такий аналіз повинен проводитись у випадках, коли конкретні ризики мали вплив на права та свободи суб'єктів персональних даних. Аналіз ризиків та розробка заходів по їх мінімізації є обов'язковими, більше того ризики з найвищим ступенем впливу повинні попередньо узгоджуватись з органами захисту даних.

Згода на обробку персональних даних напевно одна з ключових вимог перед початком їх обробки. Активна згода на обробку повинна містити чітку мету збору даних та їх подальшої обробки. Контролери в подальшому повинні мати змогу довести наявність такої згоди або заборони на перший запит, також повинна бути можливість відкликання попередньо наданої згоди. Для неповнолітніх осіб така згода повинна бути надана батьками чи опікунами, відповідним чином нотаріально завірена.

Для забезпечення належного контролю та виконання Положення в кожній організації повинен бути призначений Офіцер з захисту персональних даних (Data protection officer). Вимоги до визначення Офіцерів:

• Обов'язково повинні бути визначені для усіх публічних органів, окрім судів, які діють згідно власних повноважень;

• Повинні бути визначені, якщо контролер або процесинг містить:

– обробку операцій, які за своєю натурою, типом та/або метою, вимагають регулярного та систематичного моніторингу суб'єктів даних у великих об'ємах;

– обробку у великому об'ємі особливих категорій (таких, як расова або етнічна приналежність, релігія чи етичні норми, політичні погляди, релігійні та філософські переконання, участь в професійних спілках, генетичні дані, біометричні дані для унікального розпізнавання фізичної особи, дані про здоров'я або дані, які стосуються сексуального життя особи чи сексуальної орієнтації) та персональних даних, які стосуються кримінальних зізнань та звинувачень [4].

Офіцер з захисту персональних даних (DPO) має схожі функції як Офіцер комплаєнсу, проте це різні позиції. DPO повинен володіти достатніми знаннями та навичками управління IT процесами, мати розуміння роботи внутрішніх інформаційних систем компанії та механізмів обробки ними даних, бути спеціалістом в сфері безпеки даних (включно з реакцією на кібер-атаки) та інших критичних для бізнесу процесах, які межують із зберіганням, обробкою та передачею персональних та інших вразливих даних. Комплекс навичок вимагає також охоплення юридичної частини захисту даних, включно зі знанням законодавчих актів щодо даного питання. Моніторинг за роботою DPOs буде в більшій мірі відповідальністю регулятора, аніж Ради Правління організації, яка найняла DPO. Призначення DPO у великих організаціях буде досить складним викликом для Правління та для самого фахівця. Існує безліч проблем, пов'язаних з людськими факторами та з підходом до управління, які організації та приватні компанії повинні будуть врахувати під час прийняття рішення щодо створення такої посади та призначення на неї відповідного фахівця. Додатково DPO повинен буде створити свою власну команду супроводу та також повинен відповідати за їхній професійний розвиток в подальшому, оскільки вони повинні бути незалежними від організації, яка їх найняла, бути «міні-регулятором» всередині організації. Європейський Союз видав окремим документом Керівництво для Офіцерів з захисту персональних даних (16/EN WP 243 від 12 грудня 2016) [2].

Наступним важливим моментом є порушення в безпеці персональних даних (data breaches). Згідно нових вимог – контролер буде нести юридичну відповідальність за вчасне повідомлення регулюючого органу. Звітування про порушення не є суб'єктом будь-яких винятків та повинне бути виконане в межах 72 годин від дати такого порушення. Фізичні особи також повинні бути повідомлені якщо таке порушення будь-яким чином негативно впливає на них. Під порушеннями розуміються будь-якого роду крадіжки персональних даних, витік персональних даних, інформація про можливу компрометацію даних та інші супутні та/чи подібні інциденти.

Тепер трішки детальніше про санкції, які можуть бути застосовані до контролера:

– Попередження в письмовій формі за невідповідність вимогам GDPR, якщо таке порушення є першим та неумисним;

– Регулярні періодичні аудити з захисту даних;

– Штраф до 10 мільйонів євро або до 2% річного міжнародного обороту за поточний рік, залежно від того, яка сума буде більшою;

– Штраф до 20 мільйонів євро або до 4% річного міжнародного обороту за поточний рік, залежно від того, яка сума буде більшою [5].

Останнім і напевно найскладнішим у впровадженні правилом GDPR буде, так зване, «Право на видалення» (Right to erasure). Попереднє «право бути забутим» тепер замінено жорсткішим правом на видалення, яке визначає GDPR. По своїй суті це правило забезпечує суб'єктам персональних даних вимагати видалити персональні дані, які стосуються їх або будь-яким чином не відповідають вимогам законодавства, в тому числі, якщо порушують цілі використання, зазначені у Згоді, або у випадках, коли законні інтереси Контролера перетинаються з інтересами суб'єкта та його фундаментальними правами та свободами, забезпеченими законодавством з питань захисту персональних даних.

Висновки з проведеного дослідження. Підсумовуючи, можна сказати, що нові вимоги Євросоюзу в сфері захисту даних є значно жорсткіші і з точки зору самих вимог, і з точки зору відповідальності за їх порушення. На кінець 2016 року повне впровадження GDPR для компаній з кількістю клієнтів більше ніж 100 тисяч коштувало більше 90 тис. євро, залежно від рівня консалтингової компанії, де такі послуги замовлялися. Однозначно забезпечення комплаєнсу всім вимогам власноруч компаніям обходиться значно дешевше, проте на українському ринку фахівців за даною сферою є дуже мало і, відповідно, таке впровадження затягується в часі, що є критичним, оскільки повністю Положення вступає в силу вже в 2018 році. Відповідно, для компаній, які працюють з даними громадян Євросоюзу, потрібно вже мати детальний план проекту та визначені пріоритети, людей та ресурси для роботи в напрямку захисту персональних даних клієнтів.

Бібліографічний список

1. Boardman Ruth Guide to the General Data Protection Regulation / Ruth Boardman, James Mullock, Ariane Mole // Twobirds [Електронний ресурс]. – Режим доступу : https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en.

2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal of the European Union [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

3. Guidelines on Data Protection Officers ('DPOs') № 16 / EN WP 243 // Official Site of European Commission [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

4. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

5. Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law // White & Case LLP [Електронний ресурс]. - Режим доступу : https://www.whitecase.com/publications/article/unlocking-eu-general-data-protection-regulation-practical-handbook-eus-new-data.

6.Про банки і банківську діяльність : Закон України № 2121-III від 07.12.2000 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2121-14.

7.Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України № 383-18 від 03.07.2013 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/383-18.

8.Про захист персональних даних : Закон України № 2297-17 від 01.06.2010 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2297-17.

References

1. Boardman, Ruth, Mullock, James and Mole, Ariane (2016), "Guide to the General Data Protection Regulation", available at: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en (access date April 01, 2017).

2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (access date April 01, 2017).

3. Guidelines on Data Protection Officers ('DPOs') № 16 / EN WP 243, available at: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf (access date April 01, 2017).

4. 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, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (access date April 01, 2017).

5. Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law (2016), available at: https://www.whitecase.com/publications/article/unlocking-eu-general-data-protection-regulation-practical-handbook-eus-new-data (access date April 01, 2017).

6. Verkhovna Rada Ukrainy (2000), *Pro banky i bankivsku diialnist* [On Banks and Banking], Zakon Ukrainy dated 07.12.2000 no. 2121-III, available at: http://zakon2.rada.gov.ua/laws/show/2121-14 (access date April 01, 2017).

7. Verkhovna Rada Ukrainy (2013), *Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo udoskonalennia systemy zakhystu personalnykh danykh* [About changes to some normative acts of Ukraine concerning improvement of personal data protection system], Zakon Ukrainy dated 03.07.2013 no. 383-18, available at: http://zakon2.rada.gov.ua/laws/show/383-18 (access date April 01, 2017).

8. Verkhovna Rada Ukrainy (2010), *Pro zakhyst personalnykh danykh* [About personal data protection], Zakon Ukrainy dated 01.06.2010 no. 2297-17, available at: http://zakon2.rada.gov.ua/laws/show/2297-17 (access date April 01, 2017).

Андрушків І.П., Мушинський Б.М. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ: НОРМАТИВНІ ВИМОГИ УКРАЇНИ ТА ЄВРОПЕЙСЬКОГО СОЮЗУ

Мета - аналіз нормативної бази, яка регулює питання захисту персональних даних, наведення основних прикладів використання законодавства на українському ринку, виділення найпріоритетніших розділів нового положення ЄС із захисту персональних даних (GDPR) та окреслення рекомендацій по впровадженню GDPR у порівнянні з існуючою Директивою із захисту персональних даних ЄС.

Методика дослідження. В основу досліджень роботи покладені як загальнонаукові (аналіз, спостереження), так і спеціальні методи пізнання. Методи аналізу і спостереження використані для дослідження проблем при впровадженні вимог нового законодавства ЄС. Методи пізнання використані для обґрунтування важливості відповідності до вимог законодавства з питань захисту даних.

Результати. Висвітлено основні вимоги з питань захисту персональних даних в Україні, законодавчі акти, які регулюють цю сферу, та органи, які відповідають за контроль. Проаналізовано основні законодавчі вимоги Європейського Союзу у сфері захисту персональних даних. Виділено найважливіші відмінності у порівнянні з існуючим законодавством та новими вимогами. Досліджено Загальне положення про захист персональних даних та надано рекомендації по впровадженню найпріоритетніших напрямків, з детальним поясненням спірних

моментів. Визначено наслідки, які може мати невідповідність вимогам нового законодавства для компаній, що працюють з персональними даними користувачів ЄС.

Дослідження може бути використане як практичне керівництво із впровадження GDPR або приведення у відповідність до найкращих світових практик структуру та політику компанії у питаннях захисту персональних даних.

Представлено варіанти впровадження GDPR та надано експертну оцінку по організації роботи та проекту, який дозволить вчасно та в повній мірі впровадити законодавчі зміни.

Наукова новизна. Розроблено рекомендації по впровадженню сучасних підходів до захисту персональних даних. Набули подальшого розвитку пропозиції щодо приведення у відповідність до найкращих світових практик структури та політики компанії у питаннях захисту персональних даних.

Практична значущість. Результати дослідження можуть бути запропоновані для впровадження у діяльності банків та інших фінансових організацій, що сприятиме ефективному управлінню інформаційною безпекою.

Ключові слова: ризик-менеджмент, кібер-безпека, інформаційні системи, програмне забезпечення, витік даних, персональні дані, захист даних, чутливі дані, GDPR.

Andrushkiv I.P., Mushynskyi B.M. PERSONAL CUSTOMER'S DATA PROTECTION: NORMATIVE REQUIREMENTS IN UKRAINE AND EUROPEAN UNION

Purpose is to analyze a normative framework, which regulates area of personal data protection, present the main examples of legislation in use on Ukrainian market, stress up the top priority sections of a new EU General data protection regulation (GDPR), provide recommendations on GDPR implementation in comparison to existing EU Data protection Directive.

Methodology of research. The basis of the research work assigned as general (analysis, observation) and special methods of cognition. Methods of analysis and observation used to explore the problems during implementation of new legislation. Methods of cognition used for substantiation of importance to be comply with legislation in terms of data.

Findings. The research highlights the main requirements for personal data protection in Ukraine, legislation that regulates this area and supervisory bodies. Furthermore, research has detail analysis of the main legal requirements of the European Union in the field of personal data protection. Allocated the key differences, in comparison between the existing legislation and the new requirements. Analyzed General data protection regulation and provided recommendations on implementation of the highest priority areas, with a detail description of controversial moments. Also explained consequences that can have a non-compliance with the new legislation for companies which work with personal data of EU customers.

This research can be used as a practical guide for implementation of GDPR or align structure and policies in area of personal data protection to international best practice.

The research represents options of GDPR implementation and provides expert opinion on the organization of a workflow and project plan which allows completely implement the legislative changes in time.

Originality. The recommendations on introduction of modern approaches to the protection of personal data were developed. Were further developed proposals to conform to international best practice structure and policies in matters of personal data protection.

Practical value. Research results can be offered for introduction in activity of banks and other FIs, which will be instrumental in an effective management informative safety.

Key words: risk management, cyber security, information systems, software, data leakage, personal data, data protection, sensitive data, GDPR.

Андрушкив И.П., Мушинский Б.М. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ: НОРМАТИВНЫЕ ТРЕБОВАНИЯ УКРАИНЫ И ЕВРОПЕЙСКОГО СОЮЗА

Цель – анализ нормативной базы, которая регулирует вопрос защиты персональных данных, наведение основных примеров использования законодательства на украинском рынке, выделение приоритетных разделов нового положения ЕС по защите персональных данных (GDPR), предоставление рекомендаций по внедрению GDPR по сравнению с существующей Директивой по защите персональных данных ЕС.

Методика исследования. В основу исследований работы положены как общенаучные (анализ, наблюдение), так и специальные методы познания. Методы анализа и наблюдения использованы для исследования проблем при внедрении требований нового законодательства ЕС. Методы познания использованы для обоснования важности и соответствия требованиям законодательства в вопросах защиты данных.

Результаты. Освещено основные требования по защите персональных данных в Украине, законодательные акты, регулирующие эту сферу и органы, отвечающие за контроль. Проанализировано основные законодательные требования Европейского Союза в сфере защиты персональных данных. Выделены важнейшие различия по сравнению с существующим законодательством и новыми требованиями. Исследовано Общее положение о защите персональных данных и предоставлены рекомендации по внедрению приоритетных направлений, с подробным объяснением спорных моментов. Определены последствия, которые может иметь несоответствие требованиям нового законодательства для компаний, работающих с персональными данными пользователей ЕС.

Данное исследование может быть использовано как практическое руководство по внедрению GDPR или приведения в соответствие с лучшими мировыми практиками структуру и политику компании в вопросах защиты персональных данных.

Представлены варианты внедрения GDPR и предоставлена экспертная оценка по организации работы и проекта который позволит своевременно и в полной мере внедрить законодательные изменения.

Научная новизна. Разработаны рекомендации по внедрению современных подходов к защите персональных данных. Получили дальнейшее развитие предложения по приведению в соответствие с лучшими мировыми практиками структуры и политики компании в вопросах защиты персональных данных.

Практическая значимость. Результаты исследования могут быть предложены для внедрения в деятельность банков и других финансовых организаций, которая будет способствовать эффективному управлению информационной безопасностью.

Ключевые слова: риск-менеджмент, кибер-безопасность, информационные системы, программное обеспечение, утечка данных, персональные данные, защита данных, чувствительные данные, GDPR.