ВИСНОВОК
антикорупційної експертизи проєкту Закону України «Про захист персональних даних»

Картка проєкту

Ініціатор(и) проєкту акта: Чернєв Є.В., Тарасенко Т.П., Стефанчук Р.О. та ін.	Мета проєкту акта – приведення нормативного регулювання України у сфері захисту персональних даних у відповідність до нових міжнародних стандартів у цій сфері, які передбачені у Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року та Регламенті Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС	Проєкт Закону (№ 5628 від 07.06.2021) очікує розгляду

Резюме антикорупційної експертизи

Національне агентство опрацювало проєкт Закону, розроблений на виконання Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (далі – Загальний регламент про захист даних), та ідентифікувало у законопроєкті корупціогенні фактори.

Основним корупціогенним фактором проєкту Закону є надмірна кількість правових конструкцій оціночного характеру та правових невизначеностей, які можуть спричинити упереджену оцінку посадовими особами контролюючого органу (Національної комісії з питань захисту персональних даних та доступу до публічної інформації) виконання/невиконання вимог законопроєкту контролерами та операторами персональних даних.

Також проєкт Закону містить низку положень, які можуть на практиці призвести до обмеження свободи журналістської діяльності, яка є важливою передумовою розбудови громадянського суспільства та складовою загальнодержавної антикорупційної інфраструктури.

Опис виявлених корупціогенних факторів

Використання правових конструкцій оціночного характеру. Нечітка, з порушенням принципу юридичної визначеності, регламентація прав, обов'язків чи відповідальності юридичних та фізичних осіб

1. У проєкті Закону використовується значна кількість правових конструкцій оціночного характеру, а також формулювань, які містять правову невизначеність.

Зокрема, такі конструкції та формулювання використовуються при встановленні:

1) підстав для обробки персональних даних, а також в інших випадках: «життєво важливі інтереси» (п. 4 ч. 1 ст. 5, п. 3 ч. 2 ст. 7, п. 6 ч. 1 ст. 48, п. 4 ч. 2 ст. 54, п. 3 ч. 1 ст. 63); «крім випадків, коли такі інтереси не переважають інтереси або основоположні права та свободи суб'єкта персональних даних» (п. 6 ч. 1 ст. 5);

2) вимог до надання згоди на обробку персональних даних: «ствердна дія чи поведінка, яка однозначно вказує на…» (п. 4 ч. 1 ст. 6); «будь-яка інша інформація, необхідна для забезпечення чесної та прозорої обробки персональних даних» (п. 5 ч. 5 ст. 6); «розумних заходів» (ч. 10 ст. 6).

Оскільки обов'язок доведення факту надання суб'єктом персональних даних згоди на обробку його даних з дотриманням вимог, передбачених ст. 6, покладається на контролера (ч. 12 ст. 6), існує особлива важливість однозначного розуміння вказаних категорій та формулювань;

3) особливих вимог до обробки персональних даних (чутливих персональних даних): «явна згода» (п. 1 ч. 2 ст. 7); «необхідна в цілях значного суспільного інтересу у випадках, передбачених законом, за умови, що такий закон є пропорційним відносно цілі, яка переслідується, враховує принцип поваги до суті права на захист персональних даних та передбачає належні та відповідні засоби захисту основоположних прав та інтересів суб'єкта персональних даних» (п. 7 ч. 2 ст. 7); «є пропорційним відносно мети, яка переслідується, та враховує принцип поваги до суті права на захист персональних даних та передбачає належні та відповідні засоби захисту основоположних прав та інтересів суб'єкта персональних даних» (п. 10. ч. 2 ст. 7); «є пропорційним відносно легітимної цілі, яка переслідується, враховує принцип поваги до суті права на захист персональних даних та передбачає належні та відповідні засоби захисту основоположних прав та інтересів суб'єкта персональних даних» (ч. 2 ст. 11);

4) загальних обов'язків контролера та оператора: «належні технічні та організаційні заходи» (ч. 1 ст. 28); «у разі необхідності» (ч. 3 ст. 28);

5) вимог до реєстрації операцій з обробки персональних даних: «обробка персональних даних може становити ризик порушення прав і свобод суб'єкта персональних даних» (п. 1 ч. 4 ст. 34);

6) вимог до безпеки обробки персональних даних: «належні заходи технічного та організаційного характеру для забезпечення належної безпеки обробки персональних даних такого рівня, який є співмірний ризику обробки персональних даних для прав і свобод суб'єктів персональних даних із дотриманням принципу пропорційності» (ч. 1 ст. 35); «регулярне тестування» (п. 4 ч. 1 ст. 35) «розумні строки» (ч. 3 ст. 35).

Вказані правові конструкції використовуються при визначенні обов'язків/вимог до контролера персональних даних (далі – контролер) та оператора персональних даних (далі – оператор). Дотримання цих вимог буде перевірятися контролюючим органом (Національною комісією з питань захисту персональних даних та доступу до публічної інформації), у зв'язку з чим їх правова невизначеність та оціночний характер можуть створити корупційні ризики, пов'язані з можливістю упередженої оцінки посадовими особами

контролюючого органу виконання/невиконання вказаних вимог контролерами та операторами.

Рекомендації НАЗК:

визначити у проєкті Закону інтереси, які належать до життєво важливих;

унормувати чіткий механізм/алгоритм встановлення випадків, коли легітимний інтерес контролера або третьої особи не переважатиме інтересів або основоположних прав та свобод суб'єкта персональних даних (п. 6 ч. 1 ст. 5 проєкту Закону);

визначити дію чи поведінку, яку можна кваліфікувати як ствердну для цілей п. 4 ч. 1 ст. 6 проєкту Закону;

встановити виключний перелік інформації, яка необхідна для забезпечення чесної та прозорої обробки персональних даних, або чіткі критерії для її визначення (п. 5 ч. 5 ст. 6 проєкту Закону);

визначити алгоритм віднесення заходів до категорії «розумних» (ч. 10 ст. 6 проєкту Закону);

встановити критерії для віднесення згоди до «явної» (п. 1 ч. 2 ст. 7 проєкту Закону);

чітко визначити критерії обробки персональних даних, про яку йдеться у пп. 7, 10 ч. 2 ст. 7 проєкту Закону;

чітко визначити умови, за яких допускається оприлюднення матеріалів відеозйомки, кінозйомки або фотозйомки (ч. 2 ст. 11 проєкту Закону);

встановити критерії для віднесення технічних та організаційних заходів до «належних» (ч. 1 ст. 28, ч. 1 ст. 35 проєкту Закону);

визначити періодичність оновлення технічних та організаційних заходів, про які йдеться у ч. 3 ст. 28 проєкту Закону;

унормувати чіткі критерії/випадки, у разі настання яких обробка персональних даних може становити ризики порушення прав і свобод суб'єкта персональних даних (п. 1 ч. 4 ст. 34 проєкту Закону);

встановити періодичність тестування та оцінки ризиків обробки персональних даних, що передбачаються у п. 4 ч. 1, ч. 3 ст. 35 проєкту Закону.

2. У ч. 1 ст. 41 проєкту Закону визначено, що контролер та оператор зобов'язані призначити відповідальну особу з питань захисту персональних даних у випадку, якщо основна діяльність контролера або оператора:

полягає у обробці персональних даних, яка за своїм характером, обсягом та/або її ціллю вимагає регулярного, систематичного та широкомасштабного моніторингу дій або бездіяльності суб'єктів персональних даних (п. 2);

полягає або пов'язана з широкомасштабною обробкою персональних даних (п. 3);

полягає або пов'язана з обробкою персональних даних, визначених ст. 7 (п. 4).

Водночас при визначенні необхідності призначення такої відповідальної особи використовуються оціночні категорії («систематичний та широкомасштабний моніторинг», «широкомасштабна обробка»), які не розкриті у проєкті Закону, що може спричинити довільне суб'єктивне та упереджене

тлумачення вищезазначених норм контролюючим органом. Подібне словосполучення «широкомасштабний аналіз» використовується і у п. 1 ч. 3. ст. 39 проєкту Закону.

Враховуючи те, що призначення відповідальної особи з питань захисту персональних даних вимагатиме додаткових ресурсів, у тому числі фінансових, контролер не буде зацікавлений у такому призначенні, а використання оціночних категорій створюватиме корупційні ризики при тлумаченні вказаних вимог ст. 41 проєкту Закону контролюючим органом.

Рекомендації НАЗК:

у проєкті Закону:

чітко визначити випадки, які вказуватимуть на необхідність призначення контролером та оператором відповідальної особи з питань захисту персональних даних;

встановити чіткі критерії для визначення змісту категорій «систематичний та широкомасштабний моніторинг», «широкомасштабна обробка», «широкомасштабний аналіз».

3. Відповідно до ч. 1 ст. 42 проєкту Закону суб'єкт владних повноважень може призначити особу на посаду відповідальної особи з питань захисту персональних даних, якщо така особа успішно пройшла кваліфікаційний іспит і отримала сертифікат.

При цьому законопроєкт не унормовує механізм визначення суб'єкта, який проводитиме кваліфікаційний іспит та видаватиме сертифікат, а також платність/безоплатність такого іспиту та отримання сертифіката.

Крім того, у ч. 4 ст. 42 проєкту Закону передбачається, що контролюючий орган затверджує рекомендації щодо порядку складення кваліфікаційного іспиту, змісту тестових питань та практичних завдань, методику оцінювання результатів для розробки програм навчання, підвищення кваліфікації та робочих і навчальних, сертифікатних програм для закладів освіти.

Водночас у законопроєкті відсутні будь-які положення, які унормовуватимуть питання підвищення кваліфікації, зокрема щодо періодичності, платності/безплатності. Також незрозуміло, чи підвищення кваліфікації є правом чи обов'язком відповідальної особи.

Окремо необхідно звернути увагу на те, що врегулювання механізму проведення кваліфікаційного іспиту та отримання сертифіката має нормативний характер, а тому використання терміна «рекомендації» є недоречним.

Вищезазначені правові невизначеності можуть спричинити виникнення корупційних ризиків у механізмі проведення кваліфікаційного іспиту та отримання сертифіката, який визначатиме контролюючий орган.

Також слід врахувати те, що у ст.ст. 37 - 39 («Співробітник з питань захисту даних») Загального регламенту про захист даних не передбачається необхідність складення кваліфікаційного іспиту та отримання сертифіката для співробітника з питань захисту даних.

Рекомендації НАЗК:

розглянути можливість доцільності виключення вказаних вимог або, у разі необхідності, їх запровадження;встановити у проєкті Закону механізм визначення суб'єкта, який проводитиме кваліфікаційний іспит та видаватиме сертифікат, а також платність/безоплатність такого іспиту та отримання сертифіката;

у ч. 4 ст. 42 проєкту Закону слова «рекомендації щодо порядку» замінити словом «порядок»;

унормувати питання щодо необхідності проходження підвищення кваліфікації, зокрема її періодичності.

Інші зауваження

4. У ч. 1 ст. 15 проєкту Закону пропонується встановити, що окремі вимоги до обробки персональних даних не поширюватимуться на журналістську чи творчу діяльність, а саме: положення п. 1 ч. 1 ст. 4 щодо принципів добросовісності та прозорості, пп. 4 і 6 ч. 1 ст. 4, ст.ст. 18 - 27, ст. 34, ст.ст. 36 - 40.

Водночас на обробку персональних даних при здійсненні журналістської чи творчої діяльності поширюється широке коло інших вимог – пп. 2, 5, 7 ч. 1 ст. 4 «Принципи обробки персональних даних», ст. 28 «Загальні обов'язки контролера та оператора», ст. 29 «Захист персональних даних за проектуванням та за замовчуванням», ст. 30 «Спільні контролери», ст. 31 «Оператор персональних даних», ст. 32 «Обробка персональних даних за дорученням контролера або оператора», ст. 33 «Представник контролера або оператора», ст. 35 «Безпека обробки персональних даних».

Аналіз проєкту Закону свідчить про те, що порівняно із Загальним регламентом про захист даних, обсяг таких вимог є значно ширшим.

Зокрема, відповідно до ст. 85 Загального регламенту про захист даних з метою забезпечення «свободи вияву поглядів та свободи інформації» вимоги щодо обробки даних, що здійснюється для цілей журналістики чи творчої діяльності, не поширюються, в тому числі на ст. 5 «Принципи опрацювання персональних даних» (тобто всі принципи без винятків), ст. 25 «Захист даних за призначенням і за замовчуванням», ст. 26 «Спільні контролери», ст. 27 «Представники контролерів або операторів, які не мають осідків у Союзі», ст. 28 «Оператор», ст. 32 «Безпека опрацювання».

Крім того, ч. 2 ст. 15 проєкту Закону передбачає, що такий виняток може бути застосовано лише за умови, якщо контролер, який виконує обробку персональних даних (журналіст), обґрунтовано вважає, що оприлюднення інформації здійснюється в суспільних інтересах, а шкода від оприлюднення такої інформації не переважає суспільного інтересу в її отриманні.

Формулювання зазначених умов містить оціночні категорії та може спричинити ускладнення у здійсненні журналістської діяльності.

Наразі особливо важливим є забезпечення гарантій недоторканності свободи обробки інформації для цілей журналістики. Саме журналістська

діяльність, у тому числі діяльність «журналістів-розслідувачів», є важливим елементом антикорупційної інфраструктури, дієвим способом викриття корупційних практик, порушення вимог фінансового контролю, конфлікту інтересів.

Враховуючи викладене, обмеження правових гарантій на свободу вияву поглядів та свободу інформації для цілей журналістської і творчої діяльності є корупціогенним фактором, який зумовлює необхідність доопрацювання проєкту Закону у цій частині.

Рекомендації НАЗК:

поширити винятки, що передбачені у ч. 1 ст. 15 проєкту Закону, на ст. 4 (на всі положення цієї статті), а також на ст.ст. 28 - 33, 35;

виключити положення ч. 2 ст. 15 проєкту Закону.

Висновок:

проєкт Закону містить корупціогенні фактори та потребує доопрацювання з урахуванням наданих рекомендацій.

Голова Національного агентства
з питань запобігання корупції **Олександр НОВІКОВ**