WIKI INVESTIGATION.org
Crowdsourcing Platform

Пропозиції законодавчих змін

Захист персональних даних під час публічних закупівель: проблема та шляхи її усунення

Олександр Волошин
Олена Лебеденко-Матвєкас
Людмила Арахамія
Людмила Євсєєнко
Софія Єлагіна,
Ксенія Ситинська,
Анна Хитько,
Юлія Коломієць
Ілля Сутаєв
Тетяна Дорожкіна

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Ці пропозиції (policy paper) підготовлено на основі матеріалів досліджень, які були проведені громадськими детективами Проекту «Підтримка запобігання корупції та проведення розслідувань шляхом залучення громадськості на місцевому рівні» (WikiInvestigation), що реалізується Фондом Інновацій і Розвитку та фінансується програмою Європейського Союзу «Підтримка громадянського суспільства, місцевої влади та прав людини в Україні».

Ці пропозиції до законодавчих змін націлені на захист персональних даних при проведенні публічних закупівель шляхом внесення змін до Порядку функціонування електронної системи закупівель та проведення авторизації електронних майданчиків, затвердженого Постановою КМУ від 24 лютого 2016 р. № 166

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

1. Визначення проблеми на аналізі конкретних кейсів.

Відповідно до ст. 12 ч. 3 п.1 Закону України «Про публічні закупівлі», "електронна система закупівель повинна бути загальнодоступною та гарантувати недискримінацію, рівні права під час реєстрації всім заінтересованим особам та рівний доступ до інформації всім особам, обмін і збереження інформації та документів має відбуватися з гарантуванням непорушності даних про учасників і їхніх пропозицій під час проведення процедури закупівлі та їх конфіденційність **до моменту розкриття тендерних пропозицій...**". Після розкриття тендерних пропозицій система працює за принципом "всі бачать все", [1]адже, відповідно до положень цієї ж статті, електронна система закупівель повинна забезпечувати можливість доступу до цієї інформації замовників, учасників, контролюючих органів, органу оскарження, уповноваженого органу та інших осіб відповідно до положень ЗУ "Про публічні закупівлі".

Проблема полягає в тому, що достатньо часто виникають випадки вимагання Замовниками державних закупівель від потенційних учасників документів, які можуть містити конфіденційну інформацію, яка після розкриття тендерних пропозицій стає загальнодоступною.

Юридично дане питання врегульовано в ЗУ "Про публічні закупівлі", так, відповідно до ст. 27 ч. 2, "Під час розкриття тендерних пропозицій автоматично розкривається вся інформація, зазначена в пропозиціях учасників, та формується перелік учасників у порядку від найнижчої до найвищої запропонованої ними ціни/приведеної ціни. **Не підлягає розкриттю інформація, що обґрунтовано визначена учасником конфіденційною**. Конфіденційною не може бути визначена інформація про запропоновану ціну, інші критерії оцінки, технічні умови, технічні специфікації та документи, що підтверджують відповідність кваліфікаційним критеріям відповідно до статті 16 і вимогам, установленим статтею 17 цього Закону".

Однак, при тому, що можливість обґрунтовано визначати інформацію конфіденційною прямо прописана в ЗУ "Про публічні закупівлі" (ч.2 ст. 27), оператори авторизованих електронних майданчиків фактично надають змогу надавати інформації статусу конфіденційної лише для закупівель, очікувана вартість яких перевищує суму, еквівалентну 133 тисячам євро для товарів і послуг та 5150 тисячам євро - для робіт і які обов'язково додатково оприлюднюються на веб-порталі Уповноваженого органу англійською мовою.

1 ProZorro рекомендує бізнесу відстоювати право на обґрунтований запит персональних даних [Електронний ресурс]. − Режим доступу: https://prozorro.gov.ua/news/prozorro-rekomenduye-biznesu-vidstoyuvati-pravo-na-obgruntovanij-zapit-personalnih-danih

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

Таким чином, відсутність інструментів для надання документам статусу конфіденційного під час підготовки тендерної документації порушує гарантовані ЗУ “Про публічні закупівлі” права учасників державних закупівель.

Додатково особливості функціонування електронної системи закупівель регулюються Порядком функціонування електронної системи закупівель та проведення авторизації електронних майданчиків, затвердженого Постановою КМУ від 24 лютого 2016 р. № 166 (далі - Порядок).

Так, відповідно до ч. 7 Порядку, “Оператор авторизованого електронного майданчика **повинен забезпечити можливість проведення передбачених Законом процедур закупівель** в електронній системі закупівель залежно від рівня акредитації, та відповідність авторизованого електронного майданчика вимогам, визначеним у пунктах 8-10 цього Порядку. Оператор авторизованого електронного майданчика повинен у разі внесення змін до законодавства у сфері закупівель та/або прийняття нових нормативно-правових актів **привести у місячний строк з дня набрання ними чинності функціональні характеристики та можливості авторизованого електронного майданчика у відповідність з такими змінами та актами**”.

Оскільки ЗУ “Про публічні закупівлі” передбачає можливість надання інформації статусу конфіденційної - подібна функція має бути доступна для користувачів Операторів авторизованих електронних майданчиків.

Відповідно до п. 11. Порядку, “підключення електронних майданчиків до електронної системи закупівель здійснюється протягом 10 робочих днів після оприлюднення рішення щодо авторизації (попередньої авторизації) електронного майданчика та **здійснення тестування на відповідність вимогам, встановленим у пунктах 8 і 9 цього Порядку**. Тестування проводиться адміністратором. Адміністратор повинен здійснити тестування усіх електронних майданчиків, які подали за встановленою цим Порядком процедурою заявку на авторизацію електронного майданчика”.

Таким чином, Адміністратор системи електронних закупівель (Відповідно до Наказу мінекономрозвитку від 18.03.2016 N 4732, Адміністратором системи електронних

2 Наказ Мінекономрозвитку від 18.03.2016 №473 "Про визначення веб-порталу Уповноваженого органу з питань закупівель у складі електронної системи закупівель та забезпечення його функціонування" [Електронний ресурс]. − Режим доступу: http://me.gov.ua/LegislativeActs/Detail?lang=uk-UA&id=c508aec9-714d-46d5-8a23-ac1fa0a7c1b2&title=NakazMinekonomrozvitkuVid18-03-2016-473-proViznachenniaVebportaluUpovnovazhenogoOrganuZPitanZakupivelUSkladiElektronnoiSistemiZakupivelTaZabezpechenniaYogoFunktsionuvannia-

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

закупівель виступає ДП “Прозорро”), відповідальний за тестування на відповідність електронних майданчиків встановленим вимогам законодавства. Однак, у пунктах 8 та 9 Порядку, вимоги забезпечити всіх учасників закупівель можливістю надавати інформації статусу конфіденційної, не встановлено.

Натомість, у пп.4 п. 8 Порядку, вказано лише на необхідність “захисту інформації про публічні закупівлі та захисту конфіденційної інформації від несанкціонованого доступу”. Подібне трактування можна зрозуміти в контексті забезпечення **захисту конфіденційності до відкриття тендерних пропозицій**, тому воно не відображає повністю всіх встановлених ЗУ “Про публічні закупівлі” вимог щодо забезпечення конфіденційності. Відповідно до пп. 10 п. 9 Порядку, “В електронній системі закупівель повинна бути створена комплексна система захисту інформації з підтвердженою відповідністю згідно з **вимогами законодавства у сфері захисту інформації**”. Одним із Законів України у сфері захисту інформації можна вважати ЗУ “Про захист персональних даних”, відповідно до ст.8 ч.2 п.10 якого, суб'єкт права персональних даних **має право “вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди**”. Реалізація даного права суб'єкта права персональних даних ніяким чином не здійснюється під час участі у системі електронних закупівель.

Вищезазначені особливості функціонування та законодавчого регулювання системи електронних закупівель призводять до низки негативних наслідків. Так, якщо Постачальник бере участь у закупівлі, в якій Замовник вимагає фотокопії його паспорту/ідентифікаційного коду тощо, значить, він добровільно погоджується на розміщення своїх персональних даних у відкритому доступі системи. Проблема полягає в тому, що відмова від надання таких даних часто кваліфікується як подання неповного пакета документів, а можливість надання цим даним статусу конфіденційних не забезпечується системою. Дійсно, жодним Законом не передбачена необхідність оприлюднення копій паспорту або РНОКПП для участі у тендері і на офіційному сайті системи електронних закупівель, часто публікуються застереження[3] для учасників стосовно відсутності зобов'язання надавати такі дані та рекомендації стосовно вирішення цієї проблеми. Однак учасники рідко дотримуються даних рекомендацій, оскільки оскарження неправомірних вимог замовників вимагає витрачання часу та ресурсів, а отже - знижує ефективність їх роботи. Як наслідок - випадки шахрайства з використанням персональних даних набувають загального поширення.

Так, в жовтні 2018 року бізнесмен Валерій Яковенко заявив, що став жертвою шахраїв, які оформили кредит на його ім'я на сайті Moneyveo.UA

У своєму пості на Фейсбук автор повідомив, що фотокопії документів з його

3 Як Постачальнику захистити свої персональні дані [Електронний ресурс]. − Режим доступу: https://infobox.prozorro.org/articles/yak-postachalniku-zahistiti-svoji-personalni-dani

Цей проект фінансується Європейським союзом
Цей проект реалізується Фондом Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

персональними даними зловмисники взяли із системи ProZorro[4].

Бізнесмен заявив, що людей, які постраждали від аналогічних схем шахрайста з документами багато.

Більшість з них - підприємці, які працюють на платформі державних закупівель[5], керівники фірм та відповідальні особи, які вимушені публікувати фотокопії своїх паспортів та РНОКПП у відкритому доступі.

При цьому, видалити фотокопії своїх персональних даних, після розкриття тендерної документації неможливо навіть за письмовими зверненнями до ДП «Прозорро» – ці дані завжди будуть знаходитись у відкритому доступі для всіх.

Особливо гостро постає необхідність захисту персональних даних у системі ProZorro з огляду на можливості автоматизації процесу завантаження інформації, яку розміщують учасники тендерів. Так, всі документи, необхідні для участі в державних закупівлях, завантажуються за допомогою OpenProcurement - комплексу програмних засобів з відкритим вихідним кодом, розробленим для автоматизації та оптимізації закупівель.

Використання подібного комплексу дозволяє здійснювати завантаження великих масивів інформації за допомогою використання спеціального програмного забезпечення та стандартних пошукових систем (наприклад - Google).

Так, використавши пошуковий запит “паспорт громадянина” за допомогою пошукової системи Google.com з посиланням напряму на базу даних, на якій зберігаються документи учасників державних закупівель (запит вигляду “site:https://public.docs.openprocurement.org паспорт громадянина”) - можна завантажити 256 000 файлів, більшість з яких є сканованими копіями паспортів та реєстраційних номерів облікових карток платників податків (РНОКПП)

Результат вказаного пошукового запиту від 26.07.2019 зображено на рис. 1.

4 Кредитні шахраї використовували персональні дані українців із системи ProZorro [Електронний ресурс]. − Режим доступу: https://ua.news/ua/kredytni-shahrayi-vykorystovuvaly-personalni-dani-ukrayintsiv-iz-systemy-prozorro/
5 В ДП «ПРОЗОРРО» прокоментували можливе несанкціоноване використання персональних даних учасників публічних закупівель [Електронний ресурс]. − Режим доступу: https://dozorro.org/news/v-dp-prozorro-prokomentuvali-mozhlive-nesankcionovane-vikoristannya-personalnih-danih-uchasnikiv-publichnih-zakupivel

Цей проект фінансується Європейським союзом
Цей проект реалізується Фондом Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

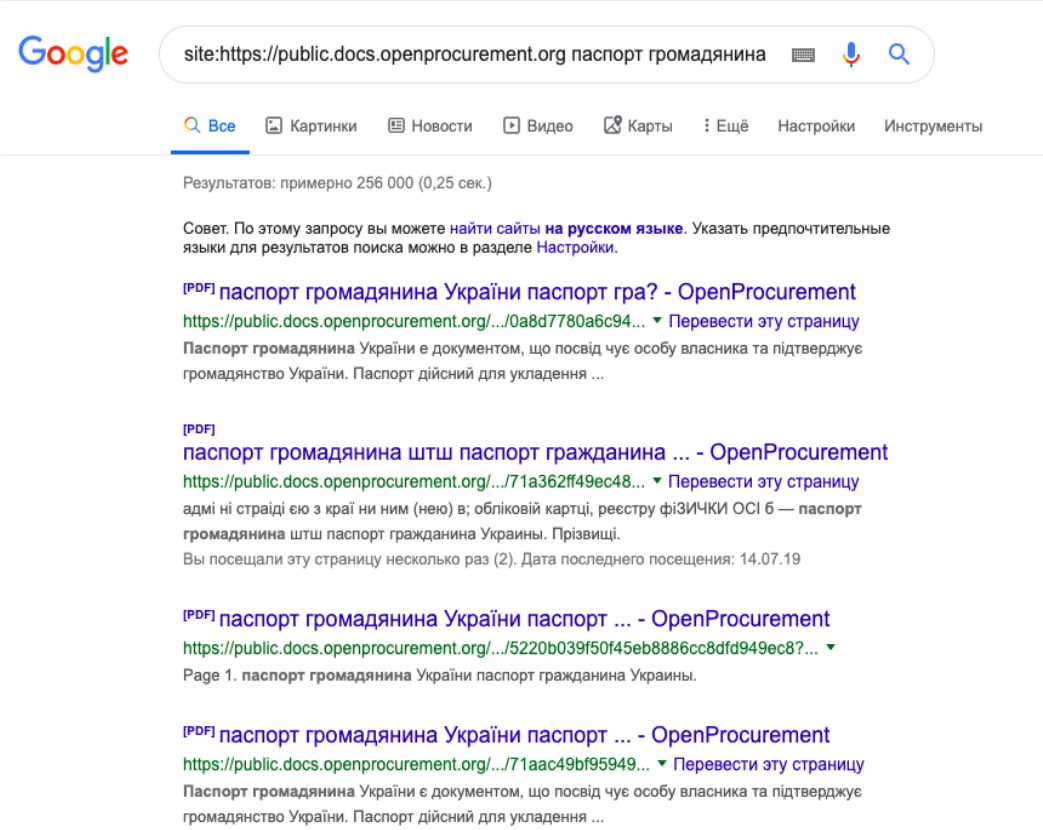

Рисунок 1. – результати пошукової видачі за запитом: «site:https://public.docs.openprocurement.org паспорт громадянина»

Використання спеціального програмного забезпечення дає змогу завантажити всі файли з пошукової видачі за лічені години. Таким чином, будь-який користувач Інтернет, може отримати доступ до персональних даних сотень тисяч українських громадян, що приймали участь у державних закупівлях.

Також, оскільки учасниками закупівель часто виступають громадяни інших країн (в т.ч. - країн Європейського Союзу), пошукові запити стосовно персональних даних іноземних громадян також дають змогу завантажити їх конфіденційні дані. Наприклад, на рис. 2 зображено пошуковий результат за запитом “site:https://public.docs.openprocurement.org united kingdom passport”.

Цей проект фінансується Європейським союзом
Цей проект реалізується Фондом Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

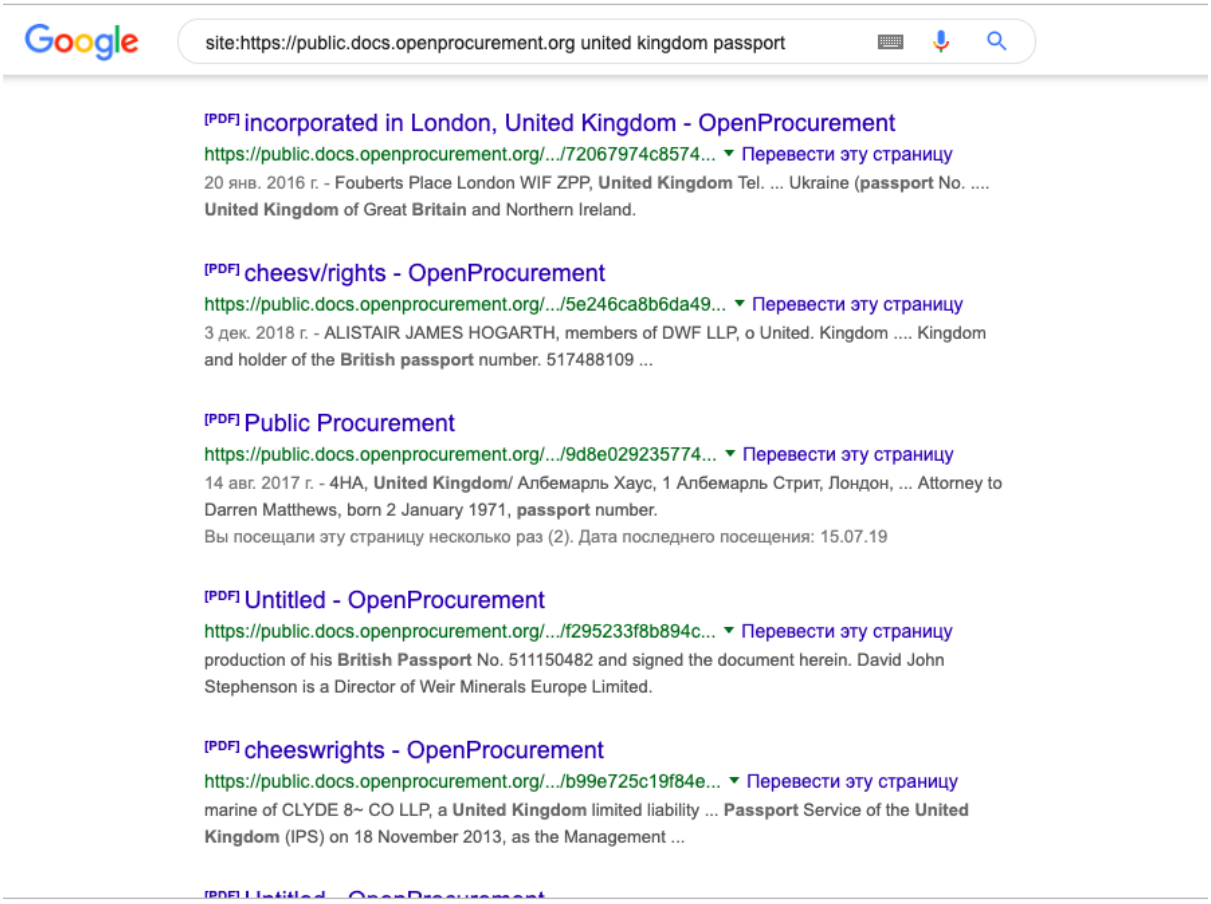

Рисунок 2. – результати пошукової видачі за запитом: «site:https://public.docs.openprocurement.org united kingdom passport»

Таким чином, навіть звичайний пошук у Google дає можливість завантажити паспорти громадян різних держав, які брали участь у державних закупівлях. Зважаючи на значне посилення відповідальності за обробку і висвітлення конфіденційної інформації, яке останнім часом спостерігається у розвинених країнах, подібна організація зберігання персональних даних може стати причиною міжнародних скандалів.

Вимога розміщувати фотокопії документів (паспортів та РНОКПП) у системі ProZorro також викликає суттєвий резонанс, скарги та обурення серед підприємців, про що можуть свідчити, наприклад, запити громадян до Міністерства економічного розвитку і

Цей проект фінансується Європейським союзом
Цей проект реалізується Фондом Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

торгівлі України, які розміщено на офіційному сайті вказаної установи.[6]

6 Офіційний сайт міністерства економічного розвитку і торгівлі України [Електронний ресурс]. − Режим доступу: http://www.me.gov.ua/InfoRez/Details?id=3b12c60f-60c0-46df-966a-a52a0e731a15&lang=uk-UA
Офіційний сайт міністерства економічного розвитку і торгівлі України [Електронний ресурс]. − Режим доступу: http://www.me.gov.ua/InfoRez/Print?id=5bd9f1bd-31c5-4890-98ce-25e44a2a9905&tagId=7758c77b-e410-44ea-a07d-37f1799e11e5&tag=ZapitiKoristuvachiv&lang=uk-UA

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

2. Міжнародний досвід

Аналізуючи питання організації проведення державних закупівель у країнах ЄС слід зазначити, що Договір про функціонування Європейського Союзу не містить окремих положень, які безпосередньо стосуються саме державних закупівель, однак вони приділяють все більшу увагу питанню захисту конфіденційності персональних даних загалом. 25 травня 2018 року набули чинності нові вимоги Європейського парламенту щодо захисту персональних даних. Правила закріплені в General Data Protection Regulation[7] (далі – GDPR). Даний документ має пряму дію та є обов'язковим для імплементації в національне законодавство усіх 28 держав-членів Європейського Союзу.

Головною метою GDPR є забезпечення гарантій захисту персональних даних громадян ЄС. Прописані у GDPR вимоги спрямовуються на посилення та уніфікацію захисту персональних даних та встановлення обов'язку захищати конфіденційність персональних даних.

Важливою особливістю регламенту є принцип екстериторіальної дії його норм (ст.3 GDPR). Отже, компаніям (в т.ч з України), які обробляють персональні дані резидентів ЄС, незалежно від місцезнаходження таких компаній, необхідно звертати увагу на вимоги GDPR для уникнення можливих негативних наслідків.

У контексті аналізу відповідності принципів роботи української державної системи публічних закупівель вимогам GDPR доцільно навести зміст наступних статей GDPR:

Відповідно до ст. 1 Регламенту: **Захист фізичних осіб під час опрацювання персональних даних є фундаментальним правом**. Статтею 8(1) Хартії фундаментальних прав Європейського Союзу («Хартія») і статтею 16(1) Договору про функціонування Європейського Союзу (ДФЄС) встановлено, що кожна особа має право на захист своїх персональних даних.

Ст. 2 зазначає, що: Принципи і норми щодо захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних передбачають, **незалежно від їхнього**

7 The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years [Електронний ресурс]. − Режим доступу: https://eugdpr.org/

Цей проект фінансується Європейським союзом
Цей проект реалізується Фондом Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

громадянства або місця проживання, дотримання їхніх фундаментальних прав і свобод, зокрема їхнього права на захист персональних даних.

У ст. 6 зазначено, що: Стрімкий технологічний розвиток і глобалізація призводять до виникнення нових труднощів для захисту персональних даних. Масштаби збирання та спільного використання персональних даних суттєво зросли. Технології дозволяють як приватним компаніям, так і публічним органам користуватися персональними даними в безпрецедентних масштабах з метою реалізації своєї діяльності. Фізичні особи дедалі частіше надають доступ до персональної інформації для громадськості та в глобальному масштабі. Технології змінили як економіку, так і суспільне життя і повинні надалі стимулювати вільний рух персональних даних у межах Союзу та передавання їх до третіх країн і міжнародних організацій, з**абезпечуючи при цьому високий рівень захисту персональних даних.**

Вказані положення містяться також у ст. 7: Такі зміни вимагають наявності міцних та більш узгоджених засад щодо захисту даних у Союзі, із запровадженням належного механізму виконання, беручи до уваги важливість формування довіри, що дозволить розвиток цифрової економіки на рівні внутрішнього ринку. **Фізичні особи повинні мати контроль щодо власних персональних даних**. Необхідно зміцнити правову та практичну визначеність для фізичних осіб, суб'єктів господарювання і органів публічної влади.

У ст.11 зазначається, що: Дієвий захист персональних даних у всьому Союзі вимагає зміцнення та детального опису прав суб'єктів даних і обов'язків осіб, які здійснюють опрацювання і приймають рішення щодо опрацювання персональних даних, а також надання рівнозначних повноважень з моніторингу і забезпечення дотримання норм щодо захисту персональних даних та застосування відповідних санкцій за порушення прав у державах-членах.

Захист, передбачений цим Регламентом, поширюється на фізичних осіб, **незалежно від їхнього громадянства чи місця проживання**, під час опрацювання їхніх персональних даних (ст.14).

Органи публічної влади, яким розкривають персональні дані відповідно до встановленого законом зобов'язання щодо виконання ними посадових функцій, такі як податкові та митні органи, служби фінансових розслідувань, незалежні адміністративні органи або органи державного регулювання фінансового ринку, відповідальні за регулювання та нагляд за фондовими ринками, не можна розглядати як одержувачів, якщо їм надають персональні дані, необхідні для проведення певного розслідування у загальних інтересах, відповідно до законодавства Союзу або держави-члена. **Запити на розкриття, які надають органи публічної влади, повинні завжди бути оформлені в письмовій формі, вмотивовані та призначені для спеціального випадку; вони не повинні впливати на всю картотеку або спричиняти взаємозалежність картотек.** Такі органи

Цей проект фінансується Європейським союзом
Цей проект реалізується Фондом Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

публічної влади повинні здійснювати опрацювання персональних даних відповідно до застосовчих норм щодо захисту даних та цілей опрацювання.(ст. 31).

Будь-яке опрацювання персональних даних повинно бути законним та правомірним. **Фізичні особи повинні бути обізнані про те, що їхні персональні дані збирають, використовують, обговорюють або іншим чином опрацьовують, а також про те, якою мірою опрацьовують чи опрацьовуватимуть персональні дані. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо опрацювання таких персональних даних були доступними і зрозумілими, з використанням чітких і простих формулювань**. Цей принцип стосується, зокрема, інформування суб'єктів даних про особу контролера та цілі опрацювання і надання подальшої інформації для забезпечення правомірного і прозорого опрацювання в частині, що стосується відповідних фізичних осіб та їхнього права на отримання підтвердження та повідомлення про ті персональні дані, які їх стосуються та підлягають опрацюванню. Фізичні особи повинні бути обізнані про ризики, правила, гарантії та права щодо опрацювання персональних даних і про те, як реалізувати свої права у зв'язку з таким опрацюванням. Зокрема, спеціальні цілі опрацювання персональних даних повинні бути прямо вираженими та законними, а також означеними на момент збирання персональних даних. Персональні дані повинні бути достатніми, відповідними та обмежуватися тим, що є необхідним для досягнення цілей, для яких їх опрацьовують. Це вимагає, зокрема, забезпечення того, що період, протягом якого зберігаються персональні дані, скорочений до абсолютного мінімуму. Персональні дані необхідно опрацьовувати, лише якщо мети опрацювання не можна досягнути розумним чином іншими засобами. Щоб забезпечити, що персональні дані не зберігаються довше, ніж це необхідно, **контролер повинен встановити часові рамки для стирання або періодичного перегляду**. Необхідно вживати всіх відповідних заходів для забезпечення виправлення або видалення неточних персональних даних. Персональні дані необхідно опрацьовувати в спосіб, що забезпечує відповідний рівень безпеки та конфіденційності персональних даних, у тому числі для запобігання несанкціонованому доступу або використанню персональних даних, а також обладнання, необхідного для опрацювання.(ст. 39).

Принципи правомірного та прозорого опрацювання вимагають, щоб суб'єкта даних було проінформовано про наявність операції опрацювання та її цілі. Контролер повинен надавати суб'єкту даних будь-яку подальшу інформацію, необхідну для забезпечення правомірного та прозорого опрацювання, враховуючи конкретні обставини та контекст, що супроводжують опрацювання персональних даних. Крім того, необхідно проінформувати суб'єкта даних про наявність профайлінгу та наслідки такого профайлінгу. У разі отримання персональних даних від суб'єкта даних, його або її також необхідно проінформувати про те, чи зобов'язаний він або вона надати персональні дані, та про наслідки ненадання таких даних. Таку інформацію можна надавати в поєднанні зі стандартизованими іконками для того, щоб навести, у видимий, доступний для розуміння та чіткий спосіб, змістовний огляд запланованого опрацювання. У разі представлення іконок у електронному форматі, вони повинні легко зчитуватися машиною. (ст. 60).

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

Суб'єкт даних повинен мати право на виправлення своїх персональних даних і «право бути забутим», якщо утримання таких даних порушує цей Регламент або законодавство Союзу чи держави-члени, яке поширюється на контролера. Зокрема, суб'єкт даних повинен мати право на видалення своїх персональних даних та припинення їхнього опрацювання, якщо персональні дані більше не є потрібними щодо цілей, для яких їх збирають або іншим чином опрацьовують, якщо суб'єкт даних відкликав свою згоду або заперечує проти опрацювання його або її персональних даних, або якщо опрацювання його чи її персональних даних іншим чином не відповідає цьому Регламенту. Таке право є доцільним, зокрема, коли суб'єкт даних надав свою згоду, будучи дитиною, та не є повністю обізнаним про ризики, пов'язані з опрацюванням, а пізніше хоче видалити такі персональні дані, особливо з мережі Інтернет. Суб'єкт даних повинен мати можливість реалізовувати таке право, незважаючи на той факт, що він більше не є дитиною. Проте подальше утримання персональних даних повинно бути законним, за необхідності, для реалізації права на свободу вияву поглядів та свободу інформації, дотримання встановленого законом зобов'язання, виконання завдання в суспільних інтересах чи офіційних повноважень, покладених на контролера, на підставі суспільного інтересу в сфері охорони суспільного здоров'я, для досягнення цілей у суспільних інтересах, цілей наукового чи історичного дослідження, статистичних цілей, або для формування, здійснення або захисту законного права вимоги.(ст. 65).

Порушення захисту персональних даних може, якщо не його не розглянути своєчасно та належним чином, призвести до нанесення фізичним особам фізичної, матеріальної та нематеріальної шкоди, такої як втрата контролю над їхніми персональними даними або обмеження їхніх прав, дискримінація, крадіжка персональних даних або шахрайство, фінансові втрати, несанкціоноване скасування використання псевдонімів, шкода репутації, втрата конфіденційності персональних даних, захищених як особисту таємницю, або будь-яка інша істотна економічна або соціальна шкода відповідній фізичній особі. **Таким чином, як тільки контролеру стає відомо про порушення захисту персональних даних, він повинен повідомити наглядовий орган про порушення захисту персональних даних без неналежної затримки та, за можливості, не пізніше ніж за 72 години після того, як йому стало про це відомо, за винятком якщо контролер може довести, згідно з принципом підзвітності, що порушення захисту персональних даних малоймовірно створить ризик для прав і свобод фізичних осіб**. Якщо неможливо здійснити таке повідомлення протягом 72 годин, у такому разі разом із повідомленням необхідно надати відомості про причини затримки; інформацію можна надати поетапно без неналежної подальшої затримки. (ст. 85).

Таким чином, особливості функціонування системи публічних закупівель в Україні порушують цілий ряд вимог GDPR (фактична неможливість контролювати та видалити свої персональні дані, які стають загальнодоступними та можуть призвести до матеріальних втрат та шахрайства).

З формальної точки зору, GDPR безпосередньо не зачіпає українське бізнес середовище. Однак, в умовах відкритих світових ринків, лібералізації торгівлі, економічної

Цей проект фінансується Європейським союзом
Цей проект реалізується Фондом Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

та інформаційної інтеграції, українські компанії не зможуть залишитися осторонь від створення єдиного європейського правового механізму захисту персональних даних. Причина тому дуже проста – для ведення бізнесу, необхідно відповідати правилам. Адже рівень санкцій, передбачений GDPR за порушення порядку захисту персональних даних настільки високий (4% річного обороту компанії або 20 мільйонів євро), що дозволити собі мати справу з компанією, яка не гарантує дотримання правил обробки персональних даних мало хто захоче. До того ж, у функціонуванні публічної системи закупівель наразі існують ймовірні випадки порушення прав громадян ЄС (оскільки їх конфіденційні дані можна завантажити у відкритому доступі).

Україна обрала європейський вектор розвитку, підписала Угоду про Асоціацію з ЄС і, робить спроби європейської інтеграції. Складно собі уявити продовження цього процесу без створення однакових з ЄС єдиних правил захисту європейських цінностей, в яких захист персональних даних, як складова права на недоторканність приватного життя, займає далеко не останнє місце.

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

3. Шляхи вирішення проблеми

Шляхи усунення проблем з доступом до персональних даних в системі державних закупівель “Прозоро” доцільно умовно розділити на 3 складових:

1. Захист від можливості здійснення автоматизованого вивантаження з використанням інструментів пошуку. Для ускладнення можливостей автоматизації пошуку та завантаження персональних даних, доцільно на програмному рівні прибрати можливість здійснення індексації пошуковими системами інформації, яку завантажують учасники електронних державних закупівель в систему електронних публічних закупівель. Програмна реалізація подібного рішення займає зазвичай декілька хвилин.

2. Додати можливість на програмному рівні обґрунтовано називати файл конфіденційним для учасників будь-якої закупівлі. При тому, що така можливість прямо прописана в ЗУ “Про публічні закупівлі” (ч.2 ст. 27), відсутність інструментів для надання документам статусу конфіденційного під час підготовки тендерної документації порушує гарантовані Законом права учасників державних закупівель. Також відсутність можливості обмежувати подібної права на обробку своїх персональних даних під час надання згоди на участь у державних закупівель порушує права учасників електронної системи державних закупівель, зазначені у ст.8 ч.2 п.10 ЗУ “Про захист персональних даних”, а саме - права суб'єкта персональних даних “10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди”. Зобов'язання додавання подібної опції юридично можна закріпити, розширивши пп.2 п.8 Порядку функціонування електронної системи закупівель та проведення авторизації електронних майданчиків, затвердженого Постановою КМУ від 24 лютого 2016 р. № 166 наступним чином (виділено напівжирним):

“2) учасникам торгів:

рівний доступ до участі в закупівлях;

підтвердження особи користувача за допомогою способів ідентифікації, визначених у пункті 3 цього Порядку, під час розміщення будь-якої інформації в електронній системі закупівель;

перевірку достовірності своїх реєстраційних даних, що надаються під час реєстрації в електронній системі закупівель та у разі зміни таких даних;

Цей проект фінансується Європейським союзом
Інновацій та Розвитку
Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

автоматичну реєстрацію усіх дій користувачів на авторизованому електронному майданчику у спеціальному журналі подій;

надіслання повідомлень учаснику та відображення їх у його кабінеті на авторизованому електронному майданчику;

надання можливості учаснику управляти документами, які були створені на одному авторизованому електронному майданчику, у разі перереєстрації учасника на іншому;

надання можливості учаснику обґрунтовано визначати інформацію, зазначену в своїй тендерній пропозиції, конфіденційною, крім інформації про запропоновану ціну, інші критерії оцінки, технічні умови, технічні специфікації та документи, що підтверджують відповідність кваліфікаційним критеріям відповідно до статті 16 і вимогам, установленим статтею 17 ЗУ "Про публічні закупівлі".

3. Забезпечити можливість видалення конфіденційної інформації, що відноситься до персональних даних, за зверненням суб'єктів персональних даних, оскільки відповідно до п.11 ч.2 ст.8 ЗУ "Про захист персональних даних", суб'єкт персональних даних має право відкликати згоду на обробку персональних даних.

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.

4. Комунікаційна стратегія

Комунікаційна стратегія може включати наступні елементи:

- Створення груп стейкхолдерів відповідно до запропонованих складових вирішення проблеми;

- Просування ідей законодавчих змін через медіа (новини, публікації, пости в соцмережах, експертні думки);

- Проведення консультацій і переговорів із низкою громадських організацій, які

займаються політиками щодо вдосконалення процедур публічних закупівель;

- Проведення “круглого столу” з даної теми.

Цей проект фінансується Європейським союзом

Цей проект реалізується Фондом Інновацій та Розвитку

Погляди, висвітлені в цій публікації, можуть не збігатися з поглядами Європейського Союзу.