



11 грудня 2025 р.

АНАЛІЗ НАКАЗУ МІНІСТЕРСТВА ЮСТИЦІЇ УКРАЇНИ

**«Про відновлення оприлюднення інформації з Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань у формі відкритих даних»
від 18 листопада 2025 р. № [3168/5](#)**

Ініціатори законопроекту

Департамент державної реєстрації Міністерства юстиції України

Загальний контекст

Наказ Міністерства юстиції України від 18 листопада 2025 р. №3168/5 ухвалено на виконання положень Закону України «Про внесення змін до Цивільного кодексу України та деяких інших законів України щодо особливостей надання відомостей публічних електронних реєстрів, держателем яких є Міністерство юстиції України, та деяких інших публічних електронних реєстрів» від 21 серпня 2025 р. № [4576-IX](#), який визначив нові правила надання даних публічних електронних реєстрів та встановив поетапне відновлення доступу до інформації, що раніше була обмежена у зв'язку з воєнним станом та ризиками національної безпеки.

Документ спрямований на відновлення оприлюднення інформації з Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємств та громадських формувань (ЄДР) у формі відкритих даних відповідно до переліку, затвердженого наказом Міністерства юстиції України «Про затвердження Переліку інформації, що підлягає оприлюдненню у формі відкритих даних, розпорядником якої є Міністерство юстиції України» від 28 березня 2016 р. № [897/5](#).

Сьогодні доступ до ЄДР залишається частково обмеженим: публічний портал відображає лише базову інформацію про юридичну особу (назва, код ЄДРПОУ, статус, керівник), але дані про місцезнаходження, історію змін, попередніх керівників, структуру власності, КБВ/бенефіціарів, види діяльності, розширені реєстраційні події та інші важливі набори недоступні.

У контексті воєнного стану та необхідності забезпечення балансу між прозорістю, захистом персональних даних та безпекою, наказ Міністерства юстиції України є важливим етапом повернення реєстраційної системи держави до відкритості й відповідності міжнародним стандартам «open data».

Документ також покладає на ДП «Національні інформаційні системи» (НІС) технічний обов'язок забезпечити реалізацію цього наказу, набрання чинності якого визначено через два місяці після дати набрання чинності Законом України «Про внесення змін до Цивільного кодексу України та деяких інших законів України щодо особливостей надання відомостей публічних електронних реєстрів, держателем яких є Міністерство юстиції України, та деяких інших публічних електронних реєстрів», що надає час для технічної та організаційної адаптації.

Суть запропонованих змін

Виключення норм, що раніше призводили до блокування оприлюднення відомостей з ЄДР у форматі відкритих даних, фактично усуває тимчасові обмеження, запроваджені в умовах пікових безпекових загроз. Таке рішення повертає законодавче регулювання до режиму відкритості, який був характерним для довоєнного періоду, та забезпечує функціонування реєстру на принципах прозорості, підзвітності та доступності інформації для громадян, бізнесу й громадських організацій. Водночас воно свідчить про готовність держави відновлювати публічність, не знижуючи рівень безпекових бар'єрів, а адаптуючи їх до сучасних умов.

Покладення на ДП «Національні інформаційні системи» технічних та організаційних завдань щодо реалізації наказу означає, що саме це підприємство відповідатиме за оновлення обчислювальної інфраструктури, налаштування та стабільність роботи інтерфейсів прикладного програмування, забезпечення коректного функціонування порталів відкритих даних, а також підтримку системи кіберзахисту Cyber Shield. Такий підхід дозволяє узгодити відновлення відкритих даних з сучасними вимогами до кібербезпеки, включно з постійним моніторингом загроз, аудитом доступів та захистом від кібератак, які в умовах воєнного стану залишаються системно високими.

У цілому документ не лише відновлює правовий режим відкритості даних ЄДР, але й інтегрує його в оновлену цифрову політику Міністерства юстиції України, що відповідає поточним викликам інформаційної безпеки та трендам державної цифрової трансформації. Наказ закладає підґрунтя для подальшої модернізації реєстрової екосистеми, поєднуючи принципи відкритості з посиленими механізмами кіберзахисту та технічної стійкості.

Таким чином, відновлення доступу до реєстрових даних відбувається у збалансований спосіб: із дотриманням міжнародних стандартів прозорості, але без ігнорування ризиків, що зберігаються в умовах триваючої агресії.

Позитивні аспекти

Україна з 2015 року входить до глобальної мережі Open Data Charter та Європейської ініціативи PSI Directive. Відкритість ЄДР є ключовим елементом для протидії корупції, перевірки діяльності юридичних осіб, належної перевірки контрагентів (KYC) та оцінки пов'язаності компаній та бенефіціарної прозорості.

Для громадських організацій, журналістів, донорів та бізнес-спільноти відновлюється можливість швидко перевіряти офіційну інформацію про: статус юридичної особи, повноваження керівників, історію змін, наявність реєстраційних ризиків. Це особливо важливо для організацій, що працюють у сфері гуманітарної допомоги та потребують підтвердження правового статусу партнерів.

Багато сервісів (YouControl, Опендатабот, VKURSI, іноземні KYC-сервіси) використовують відкриті дані. Публічність даних знижує ризики рейдерства, недоброчесної поведінки керівників, незаконних змін у реєстрах, що підвищує довіру до реєстраційних процедур.

Крім того, ЄС послідовно підтримує відкритість реєстрів та узгодження з вимогами EU Single Market Transparency та Open Data Directive (2019/1024). Наказ Міністерства юстиції України наближає нашу країну до відповідності принципам ЄС та євроінтеграційним процесам.

Негативні аспекти та ризики

Рівень безпекових ризиків у зоні воєнного стану залишається високим. Попри обґрунтованість відкриття реєстру, фактично це збільшує ймовірність отримання ворогом інформації про розташування організацій, ідентифікації керівників у прифронтових регіонах, використання даних для ворожих інформаційних та психологічних операцій та посилення кібератак на майданчики, що використовують API ЄДР.

Відновлення повного обсягу наборів даних вимагає: оновлення API, модернізації серверних потужностей, тестування системи безпеки та можливих бюджетних витрат. За сучасних умов ДП «НАІС» може бути перевантаженим обсягом технічних задач.

Потенційні ризики для безпеки керівників ОГС та гуманітарних організацій. Ідентифікація керівних осіб або юридичних адрес у прифронтових районах може підвищувати ризики переслідування чи атак.

Рекомендації щодо покращення

Для забезпечення балансу між відкритістю та безпекою доцільно розробити оновлений диференційований перелік даних ЄДР, який враховуватиме рівень чутливості інформації та сучасні безпекові ризики. Такий підхід дозволяє визначити, які дані можуть бути публічними без обмежень, які потребують часткового приховування, а які повинні оприлюднюватися лише після завершення воєнного стану або за спеціальними процедурами доступу.

Перед повним відновленням доступу до всього масиву відкритих даних необхідно провести незалежний аудит кібербезпеки ДП «НАІС» із перевіркою роботи API ЄДР, систем захисту, журналів доступу та потенційних вразливостей. Одночасно важливо гармонізувати нормативну базу, усунувши потенційні колізії між старими та новими актами (технічні регламенти, внутрішні інструкції), щоб забезпечити однозначність правозастосування.

Для окремих категорій юридичних осіб варто передбачити поетапне або відкладене оприлюднення даних, що стане безпечним компромісом між прозорістю та захистом чутливої інформації і дозволить уникнути надмірних ризиків в умовах воєнного стану.

ВИСНОВОК

Наказ Міністерства юстиції України №3168/5 від 18 листопада 2025 р., яким відновлено оприлюднення інформації з ЄДР форматі відкритих даних, є важливим кроком у поверненні державної політики до стандартів прозорості та публічності. Відкриття реєстрових даних забезпечує можливість належної перевірки контрагентів, підтримує антикорупційні механізми, сприяє ефективному фінансовому моніторингу та відновлює інструменти, якими користуються бізнес, журналісти, дослідники та організації громадянського суспільства.

Разом із тим відновлення доступу до таких даних у період воєнного стану супроводжується підвищеними безпековими ризиками, насамперед для організацій та їхніх керівників, які працюють у прифронтових районах або здійснюють гуманітарну діяльність. Публічність окремих відомостей може підвищувати вразливість цих суб'єктів до кіберзагроз, переслідувань або цілеспрямованих інформаційних атак.

У цих умовах подальша державна політика має бути спрямована на приведення системи відкритих даних у відповідність з сучасними європейськими стандартами кібербезпеки, створення гнучких механізмів захисту чутливої інформації та забезпечення балансу між прозорістю реєстрів і безпекою їхніх користувачів. Це дозволить зберегти прозорість реєстрових даних та водночас забезпечити захист тих суб'єктів, що здійснюють діяльність у чутливих або ризикових умовах.