

Звіт про результати публічного громадського обговорення проекту постанови Кабінету Міністрів України «Деякі питання надання та використання хмарних послуг та/або послуг центрів обробки даних»

1. Найменування органу виконавчої влади, який проводив обговорення:

Міністерство цифрової трансформації України.

2. Зміст питання або назва проекту акта, що виносилися на обговорення:

З метою з'ясування думки та отримання пропозицій громадськості на громадське обговорення виносився проект постанови Кабінету Міністрів України «Деякі питання надання та використання хмарних послуг та/або послуг центрів обробки даних» (далі – проект постанови), яким пропонується затвердити:

Порядок надання хмарних послуг та/або послуг центру обробки даних, пов'язаних з обробкою державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

Порядок підтвердження відповідності вимогам до надавачів хмарних послуг та/або послуг центру обробки даних та вимоги до таких надавачів;

Порядок формування та використання електронних каталогів хмарних послуг та/або послуг центру обробки даних;

Типовий договір про надання хмарних послуг та/або послуг центру обробки даних публічному користувачу та об'єкту критичної інформаційної інфраструктури.

3. Інформація про осіб, що взяли участь в обговоренні:

02.12.2024 проект постанови з аналізом регуляторного впливу оприлюднено у розділі «Регуляторна діяльність» офіційного веб-сайту Мінцифри (<https://thedigital.gov.ua>).

Зауваження та пропозиції від громадськості приймалися протягом одного місяця з дня оприлюднення проекту за адресою: 03150 м. Київ вул. Ділова, 24, e-mail: zakusylo@thedigital.gov.ua.

Під час громадського обговорення отримано пропозиції від Tilemachos Moraitis, Werner Hoellrigl, Marta Kokoszka, Maxim Ageyev, Marcin Krasuski, Американської торгівельної палати в Україні, Товариства з обмеженою відповідальністю «ГІАКЛАУД», Асоціації «Телас».

	Зміни, передбачені проектом акта	Зауваження та пропозиції, що надійшли від фізичних, юридичних осіб та їх об'єднань*	Позиція Мінцифри, обґрунтування
1.	До проекту акту в цілому.	Tilemachos Moraitis Government & Corporate Affairs Manager CELA Microsoft Greece, Cyprus, Malta, Balkans, and Ukraine 1. Обмежувальні норми довоєнного стану: як проект постанови, так і наказ ЗСЦІР імплементують довоєнні норми, встановлені Законом «Про хмарні послуги» та Законом «Про захист інформації в інформаційно-комунікаційних системах». Ці правила є вкрай обмежувальними та суттєво обмежують можливості неукраїнських постачальників хмарних послуг і центрів обробки даних, таких як Microsoft, обслуговувати українських публічних користувачів і об'єкти критичної інфраструктури. Положення вимагають локальних українських сертифікацій, у тому числі криптографічних засобів захисту даних, які не дозволяють іногороднім гіперскейлерам продовжувати надавати хмарні сервіси після закінчення воєнного стану. 2. Перехідний період : Проект постанови встановлює перехідний період до 31 березня 2025 року, протягом якого користувачі публічних хмарних послуг можуть замовляти послуги у несертифікованих провайдерів. Починаючи з 1 квітня 2025 року, лише постачальники зі списку постачальників послуг хмари та/або центрів обробки даних, які відповідають відповідним вимогам і зареєструються в SSSCIP, зможуть надавати послуги. 3. Винятки та відповідність : Процедура обробки SIR містить винятки для банків, постачальників фінансових послуг, військового та оборонного секторів. Однак незрозуміло, як ці винятки слід застосовувати з огляду на поточні винятки щодо воєнного стану.	Відхилено. Внесення наданої пропозиції не забезпечить виконання норм закону України “Про хмарні послуги”. Порядок використання хмарних послуг під час воєнного стану вже врегульовано постановою Кабінету Міністрів України від 30.12.2022 № 1500 і Законом України “Про захист інформації в інформаційно-комунікаційних системах” та не змінюється у зв'язку з прийняттям проекту акту.

		Процедура відповідності та вимоги не містять жодних винятків, що створює двозначність у поєднанні з винятком МО та резервним винятком SIR. 4. Неукраїнські провайдери: зрозуміло, що прийняття цього пакету підзаконних актів у такому вигляді, як є, суттєво обмежить надання хмарних послуг і послуг центрів обробки даних неукраїнськими провайдерами державним установам і об'єктам критичної інфраструктури після 31 березня 2025 року. різко контрастує з нашою роботою в Технологічній дорадчій раді та висловленою готовністю Міністерства DT продовжувати та надалі розширювати свою співпрацю з неукраїнськими хмарні провайдери. 5. Рекомендації: Наша поточна робота в Консультативній раді з технологій (ТАВ), яка має на меті допомогти Міністерству DT в модернізації законодавчої бази України щодо хмарних технологій і кібербезпеки, навряд чи буде завершена до кінця березня 2025 року. Тому, якщо запропонований пакет вторинних нормативних актів прийнято, можна з упевненістю припустити, що 1 квітня Microsoft та інші неукраїнські хмарні постачальники більше не зможуть продовжувати підтримувати більшість державного сектору України і будуть змушені раптово припинити співпрацю. Вважаючи, що це випадок, який жодна із зацікавлених сторін не прагне втілити в життя, ми люб'язно рекомендуємо Міністерству вжити одну з таких дій: ● Відмовитися від ухвалення запропонованого пакету підпорядкованих нормативних актів, які запровадять структуру, пов'язану з хмарою, всупереч напрямку та контексту роботи, яку виконують Міністерство DT та пов'язана з ним Технологічна консультативна рада. Навіть якби нову хмарну постанову мали прийняти до кінця березня 2025 року, запропонований пакет не сприятиме продовженню співпраці між українським урядом та неукраїнськими провайдерами хмарних послуг, які чинний воєнний стан дозволяє ще протягом 6 місяців після того, як він буде скасований.	
2.	До пункту 2 проекту постанови.	● Пропонується: Якщо незабаром прийняти запропонований пакет, слід розглянути такі	Враховано. У пункті 2 проекту постанови

		поправки: і. Включіть перехідний період набагато довший за три місяці, в ідеалі до кінця воєнного стану плюс шість місяців або принаймні до кінця 2025 року. Ймовірно, це дасть достатньо часу для Міністерства, щоб представити та прийняти нову законодавчу базу для хмарної та кібербезпеки.	слова “до 31 березня 2025 р.” замінено на слова “до 31 грудня 2025 р.”
3.	До проекту акту в цілому.	іі. Звільнення від МО має застосовуватися до всього набору документів, а не лише до процедури обробки SIR.	Відхилено. Дане питання врегульовано частиною четвертою статті 4 Закону України “Про хмарні послуги” та визначено підпунктом 2 пункту 2 проекту Порядку надання хмарних послуг та/або послуг центру обробки даних, пов’язаних з обробкою державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом (далі - проект Порядку надання).
4.	До проекту акту в цілому.	ііі. Необхідно взяти до уваги винятки з воєнного стану, передбачені Законом «Про захист інформації в інформаційно-комунікаційних системах», які далі введені в дію Постановою КМУ 1500 (Виняток з ДІЛ).	Відхилено. Не є предметом регулювання даного проекту акту. Порядок використання хмарних послуг під час воєнного стану вже врегульовано постановою Кабінету Міністрів України від 30.12.2022 № 1500 і Законом України “Про захист

			інформації в інформаційно-комунікаційних системах” та не змінюється у зв'язку з прийняттям проекту акту.
5.	До проекту акту в цілому.	iv. Положення, що обмежують постачальників хмарних послуг і центрів обробки даних українськими організаціями, наприклад, вимога вказувати код ЄДРПОУ у формах заявки, необхідно адаптувати, щоб належним чином розглядати надання хмарних послуг і послуг центрів обробки даних не українськими організаціями.	Враховано редакційно. Пункт 2 проекту Структури електронних каталогів доповнено нормою про міжнародний ідентифікаційний код юридичної особи (код LEI) та проект Типового договору (реквізити сторін) доповнено нормою щодо ідентифікаційного коду ЄДРПОУ доповнено словами “(за наявності)” та про міжнародний ідентифікаційний код юридичної особи (код LEI).
6.	До проекту акту в цілому.	Werner Hoellrigl Technology Cloud Business Execution Leader & Public Sector Leader Germany (acting) Oracle Austria GmbH DC-Tower, Donau City Straße 7 A-1220 Vienna Austria FN:38835k Handelsgericht Wien 1. Відповідність світовим стандартам Спостереження: Структура посиляється на стандарти ISO/IEC, які визнані у всьому світі. Однак акцент на національних стандартах (наприклад, ДСТУ ISO/IEC	Враховано редакційно. Пункт 21 проекту Структури електронних каталогів викладено у такій редакції: “21. Відповідність міжнародному стандарту ISO/IEC 27001 або національному стандарту іноземної країни, прийнятому відповідно до міжнародного

		27001:2023) може ненавмисно обмежити міжнародну конкуренцію та сумісність. Рекомендація: Забезпечити однакове визнання як національних, так і міжнародних стандартів (наприклад, ISO/IEC 27001, 27017 та 27018:2019). Додайте посилання на стандарти криптографії з відкритим ключем (PKCS), RSA, центри сертифікації (CA) і фреймворки, такі як FedRAMP, щоб сприяти взаємодії та залучати глобальних постачальників.	стандарту ISO/IEC 27001, або ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27018:2019 «Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII» (ISO/IEC 27018:2019, IDT).»
7.	Абзац третій пункту 8 проекту Порядку надання: “8. ... Електронні інформаційні ресурси передаються до нового надавача у повному обсязі. Витрати на проведення робіт, пов'язаних з передачею електронних інформаційних ресурсів	2. Міграція та переносимість даних Спостереження: Відповідальність за витрати, пов'язані з міграцією даних, повністю лягає на нового постачальника. Такому підходу не вистачає чіткості щодо розподілу витрат і він може стримувати постачальників від участі. Рекомендація: Чітко визначте «витрати на міграцію даних», зокрема: Вихідний трафік (вихідний трафік: публічний або приватний під L2). Надання або будівництво фізичних каналів мережі L2 для глобальних провайдерів («остання миля») Сама міграція робочого навантаження/даних.	Відхилено. Дане питання врегульовується відповідно тендерних процедур, визначених Законом України “Про публічні закупівлі”.

	несе новий надавач.”	Запровадити механізми розподілу витрат із прозорими розрахунками для забезпечення справедливості та участі. Запропонуйте спільний підхід між вихідними та вхідними провайдерами для спрощення переходів.	
8.	До проекту акту в цілому.	3. Сертифікація та тривалість відповідності Спостереження: Тривалість контракту прив'язана до дійсності сертифікаційних документів, що призводить до потенційного збільшення операційних витрат. Рекомендація: Видаліть цю залежність і введіть положення про розірвання контракту через невідповідність або визнання сертифіката недійсним. Привести механізми відповідності та сертифікації як до міжнародних стандартів, так і до існуючих українських рамок (наприклад, SSSCIP). Запропонуйте співпрацю з визнаними міжнародними організаціями для перевірки сертифікації, щоб уникнути надмірності або ризиків корупції.	Відхилено. Дана пропозиція суперечить інтересам користувача хмарних послуг. Норма про розірвання, передбачена у пункті 37 проекту Типового договору.
9.	Підпункт 3 пункту 12 проекту Порядку підтвердження відповідності: “12. Моніторинг, аудит та випробування забезпечується: ...	4. Хмарна безпека та управління інцидентами Спостереження: Вимоги безпеки передбачають суворішу частоту тестування (наприклад, щомісячне тестування вразливостей), ніж глобальні стандарти (наприклад, PCI DSS вимагає щоквартального тестування).	Враховано редакційно. У підпункті 3 пункту 12 проекту Порядку підтвердження відповідності слова “не менш ніж один раз на місяць” замінено словами “не менш ніж один раз на квартал”.

	3) регулярним (не менш ніж один раз на місяць) проведенням випробувань (тестів) для виявлення загальновідомих вразливостей системних компонентів, які використовуються для надання послуг”	Рекомендація: Узгодьте частоту тестування з найкращими міжнародними практиками та застосуйте підхід, що ґрунтується на ризиках, для критичної інфраструктури. Виділіть спільну відповідальність за безпеку хмари: Хмарні провайдери керують безпекою інфраструктури. Кінцеві користувачі несуть відповідальність за захист своїх даних і програм. Включайте посилання на визнані організації, такі як Національний центр кібербезпеки Великобританії (NCSC), і використовуйте інформацію зі звітів, як-от Oracle & KPMG Cloud Threat Reports.	
10.	До проекту постанови в цілому.	5. Гнучкість у контрактах Спостереження: У типовому контракті відсутні положення про динамічні зміни, що обмежує можливість адаптації для проектів державного сектора. Рекомендація: Забезпечте гнучкість за допомогою доповнень або замовлень на обслуговування, щоб врахувати зміни в обсязі послуг або ціноутворенні в рамках погодженого бюджету. Довідкові приклади, такі як Гнучка структура в Німеччині з окремими замовленнями учасників для забезпечення масштабованості та адаптивності.	Враховано. Пункт 25 проекту Типового договору доповнено підпунктом 4 у такій редакції: “Користувач має право: ... 4) змінювати обсяг послуг, що надаватимуться у відповідний звітний період шляхом укладення додаткової угоди.”
11.	До проекту постанови в цілому.	6. Нейтралітет постачальника та сумісність Спостереження: Покладення на електронні каталоги та централізований список постачальників може призвести до фаворитизму або прив’язки до постачальника.	Відхилено. Не є предметом регулювання проекту постанови. Порядок вибору постачальника регулюється Законом України “Про публічні закупівлі”.

		Рекомендація: Підкресліть нейтральність і прозорість у виборі постачальників і забезпечте регулярне оновлення каталогу. Запровадьте чіткі, справедливі процеси повторної сертифікації для підтримки відповідності. Підкресліть необхідність суворих стандартів сумісності, щоб уникнути залежності від одного постачальника.	Запропонована регуляція висуває загальні вимоги до всіх постачальників хмарних послуг, що бажають надавати такі послуги.
12.	До проекту постанови в цілому.	7. Пропоновані семінари та консультації Спостереження: Загальні питання в анкеті TAB і детальні письмові відповіді можуть призвести до неефективності. Рекомендація: Підтримуйте цільові семінари чи інтерв'ю, щоб розв'язати неясності, зібрати вичерпні відгуки та оптимізувати практичні ідеї.	Відхилено. Не є предметом регулювання проекту постанови.
13.	До проекту постанови в цілому.	Marta Kokoszka Principal Public Policy CEE (Central and Eastern Europe) Amazon Web Services Poland Towarowa 28 00-839 Warszawa Polska AWS паралельно працював над аналізом проекту постанови, запропонованого міністерством. Наші висновки багато в чому збігаються з висновками наших колег із Microsoft. Ми виявили кілька положень, які можуть суттєво ускладнити доступ до різноманітних хмарних сервісів в Україні. Серед них: 1) обмежувальний перехідний період для використання хмарних сервісів неукраїнських провайдерів; 2) обмеження для міжнародних хмарних провайдерів щодо реєстрації в реєстрі хмарних провайдерів.	Враховано редакційно. У пункті 2 проекту постанови слова “до 31 березня 2025 р.” замінено на слова “до 31 грудня 2025 р.” Пункт 2 проекту Структури електронних каталогів доповнено нормою про міжнародний ідентифікаційний код юридичної особи (код LEI) та проект Типового договору (реквізити сторін) доповнено нормою щодо ідентифікаційного коду

		Що ще важливіше, за відсутності більш суттєвих змін на рівні загального законодавства, запропонований проект постанови сам по собі не може вирішити основні проблеми хмарних провайдерів. Пропонується: Тому ми рекомендуємо відкласти прийняття постанови до вирішення цих питань, а потім переглянути для забезпечення відповідності оновленим законам.	ЄДРПОУ доповнено словами “(за наявності)” та про міжнародний ідентифікаційний код юридичної особи (код LEI) .
14.	Пункт 14 проекту Порядку підтвердження відповідності: “14. Надавач забезпечує відповідність міжнародному стандарту ISO/IEC 27001 або національному стандарту іноземної країни, прийнятому відповідно до міжнародного стандарту ISO/IEC 27001, або ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27018:2019	1. Визнання міжнародних стандартів інформаційної безпеки на рівні Проекту Питання: Згідно з п. 14 проекту Порядку підтвердження відповідності вимогам до постачальників хмарних послуг та/або послуг центрів обробки даних та вимогам до таких постачальників (Порядок), постачальники хмарних послуг (CSP) повинні відповідати вимогам ISO/IEC 27001 та ISO /IEC 27018:2019 на додаток до інших відповідних технічних вимог, зазначених у Процедурі та статті 8 Закону України Про захист інформації в інформаційно-комунікаційних системах № 80/94-ВР від 5.07.1994 (Закон про захист інформації). Рекомендація: Внести до пункту 14 проекту Порядку редакцію, яка дозволить альтернативно підтверджувати відповідність чинним технічним стандартам лише відповідністю міжнародним стандартам безпеки інформації (наприклад, ISO/IEC 27001 та ISO/IEC 27018:2019). Міжнародні стандарти безпеки повинні мати пріоритет над місцевими технічними вимогами з кількох вагомих причин. Ці стандарти представляють всесвітньо визнані найкращі практики інформаційної безпеки та конфіденційності, включаючи досвід міжнародних експертів і регулярно оновлюються з урахуванням нових загроз і технологій, часто частіше, ніж місцеві норми. Дотримання міжнародних стандартів забезпечує кращу взаємодію та узгодженість між глобальними хмарними службами, що приносить користь як постачальникам послуг, так і користувачам хмари. Крім того, відповідність загальновизнаним	Враховано редакційно. Пункт 21 проекту Структури електронних каталогів викладено у такій редакції: “21. Відповідність міжнародному стандарту ISO/IEC 27001 або національному стандарту іноземної країни, прийнятому відповідно до міжнародного стандарту ISO/IEC 27001, або ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27018:2019 «Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних

	«Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (РІІ) у загальнодоступних хмарах, що діють як процесори РІІ» (ISO/IEC 27018:2019, IDT).»	міжнародним стандартам може підвищити привабливість України для глобальних партнерів і транснаціональних корпорацій. Важливо, що прийняття міжнародних стандартів узгоджується з підходами Європейського Союзу, підтримуючи ширші цілі України щодо інтеграції в ЄС та гармонізації цифрового ринку. Наголошуючи на цих міжнародних стандартах, Україна може забезпечити надійну інформаційну безпеку, а також сприяти більш глобальній конкурентоспроможності та сумісності екосистеми хмарних послуг.	хмарах, що діють як процесори РІІ» (ISO/IEC 27018:2019, IDT).»
15.	Пункт 2 проекту Структури електронних каталогів: “2. Ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України або реєстраційний номер облікової картки платника податків або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили	2. Питання відповідності неукраїнським провайдером хмарних послуг та/або послуг центрів обробки даних (CSP) Питання: Пункт 2 Додатку до проекту Порядку формування та використання електронних каталогів хмарних сервісів та/або послуг ЦОД, а також п. 2 проекту Форми заяви про включення постачальників хмарних сервісів та/або даних. Послуги Центру в Переліку (Аплікаційна форма, Перелік, у відповідних випадках) передбачають, що український реєстраційний номер підприємства (код ЄДРПОУ) є обов’язковим реквізитом для CSP. Ця вимога фактично виключає неукраїнські юридичні особи з формування електронних каталогів хмарних сервісів та/або послуг центрів обробки даних, а також від включення до Переліку на тих же умовах, що й українські суб’єкти. Рекомендація: До Проекту та Форми заявки необхідно внести зміни, щоб скасувати всі вимоги щодо обов’язкового вказівки українського реєстраційного номера підприємства (коду ЄДРПОУ) з метою формування електронного каталогу хмарних сервісів та/або сервісів ЦОД та включення до Переліку. Крім того, у проекті має бути чітко зазначено, що не українські юридичні особи, які функціонують як провайдери	Враховано редакційно. Пункт 2 проекту Структури електронних каталогів доповнено нормою про міжнародний ідентифікаційний код юридичної особи (код LEI) та проект Типового договору (реквізити сторін) доповнено нормою щодо ідентифікаційного коду ЄДРПОУ доповнено словами “(за наявності)” та про міжнародний ідентифікаційний код юридичної особи (код LEI) .

	про це відповідний контролюючий орган і мають відмітку в паспорті)”. хмарних послуг (CSP), мають право формувати електронний каталог хмарних сервісів та/або послуг центрів обробки даних та включатися до Переліку за тими ж правилами, що й діють. українським суб'єктам-ПСУ. Ці зміни забезпечать рівне ставлення та можливості як для вітчизняних, так і для міжнародних CSP, сприяючи більш інклюзивному та конкурентному ринку хмарних послуг в Україні.		
16.	Абзац другий пункту 2 проекту постанови: “2. Установити, що: до 31 березня 2025 р. публічні користувачі хмарних послуг можуть ініціювати закупівлю відповідних хмарних послуг та/або послуг центрів обробки даних у надавачів хмарних послуг не включених до Переліку надавачів хмарних послуг та/або послуг центру обробки даних”	3. Короткий перехідний період до того, як правила, встановлені проектом, стануть обов’язковими для надання хмарних послуг та/або послуг центрів обробки даних клієнтам державного сектору Питання: Відповідно до п. 2 проекту публічні замовники можуть купувати хмарні послуги у ПСУ, які не включені до Переліку, лише до 31 березня 2025 року. Такого короткого перехідного періоду недостатньо для забезпечення дотримання всіх вимог. Рекомендація: продовжити перехідний період до 24 місяців, щоб постачальники послуг могли забезпечити дотримання всіх вимог і тим часом надавати хмарні послуги та/або послуги центру обробки даних клієнтам державного сектору. Довший 24-місячний період надасть CSP достатньо часу, щоб ретельно перевірити вимоги, переглянути умови обслуговування та обговорити будь-які проблеми з відповідними організаціями до досягнення повної відповідності. Цей подовжений перехідний період забезпечить провайдерам послуг широкі можливості підтвердити свої послуги та операції відповідно до необхідних вимог, водночас дозволяючи державним клієнтам отримати доступ до більш широкого спектру хмарних послуг протягом проміжного періоду. Додатковий час сприятиме більш плавному та спільному процесу відповідності, що принесе користь як постачальникам послуг, так і клієнтам державного сектору.	Враховано редакційно. У пункті 2 проекту постанови слова “до 31 березня 2025 р.” замінено на слова “до 31 грудня 2025 р.”.
17.	До проекту постанови в цілому.	Рекомендації щодо законів первинного рівня:	Відхилено. Не є предметом регулювання

		Незважаючи на те, що прийняття проекту вимагає Закон України «Про хмарні послуги» №. 2075-IX від 17.02.2022 (Закон про хмари), статус Проекту є другорядним щодо Закону про хмари та інших діючих законів України первинного рівня, які стосуються хмарних питань. Ці закони містять деякі застарілі або обмежувальні елементи, які перешкоджають належному функціонуванню хмарного сектора. Вирішення цих питань на рівні первинного законодавства має вирішальне значення перед тим, як приступити до прийняття проекту. Основні питання, які мають бути пріоритетними: (i) Обробка персональних даних Питання: Відповідно до частини третьої статті 10 Закону України «Про захист персональних даних» 2297-VI від 01.06.2010 (Закон про конфіденційність даних), розпорядником персональних даних, якщо розпорядником є державне чи комунальне утворення, може бути лише державне чи муніципальне утворення. Це положення створює необґрунтовану перешкоду для державних споживачів у виборі свого ПСУ, обмежуючи вибір державними або муніципальними установами. Рекомендація: Вилучити вищезазначене положення із Закону про конфіденційність даних. Нинішнє обмеження штучно обмежує пул потенційних CSP, знижує конкуренцію та пропозицію хмарних сервісів. Постачальники послуг приватного сектору часто лідирують у технологічних інноваціях, і обмеження державних організацій державними або муніципальними процесорами може позбавити їх доступу до передових хмарних технологій і послуг. Багато країн дозволяють державним організаціям використовувати приватні хмарні провайдери, дотримуючись суворих стандартів безпеки та захисту даних, і Україна повинна відповідати цим найкращим світовим практикам, щоб залишатися конкурентоспроможною.	проекту постанови. Зазначені пропозиції будуть враховані у подальшій роботі під час розробки інших нормативно-правових актів.
--	--	--	--

		Слід зосередитися на дотриманні суворих стандартів захисту даних і вимог до відповідності, а не на обмеженні провайдерів на основі їх публічного чи приватного статусу. Усунення цього обмеження дасть державним установам більше гнучкості у виборі найбільш підходящого CSP для їхніх конкретних потреб і вимог. Крім того, дозвіл приватним CSP обслуговувати державні організації може сприяти кращій міжнародній співпраці та обміну даними, коли це необхідно. Доступ до більш широкого спектру CSP може прискорити модернізацію публічних послуг за допомогою передових хмарних технологій. Вилучивши це положення, Україна може створити більш відкрите, конкурентоспроможне та інноваційне середовище для хмарних послуг у державному секторі, зберігаючи при цьому високі стандарти захисту даних через відповідні правила та вимоги дотримання.	
18.	До проекту постанови в цілому.	(ii) Визнання міжнародних стандартів інформаційної безпеки на рівні законів первинного рівня Проблема: відповідно до Закону про хмарні технології (стаття 8) і Закону про захист інформації (стаття 8), постачальники послуг повинні підтвердити відповідність своїх систем місцевим технічним стандартам. Поточні українські стандарти є нечіткими та застарілими, що робить непрактичним дотримання міжнародними постачальниками послуг (які працюють на основі найкращих світових стандартів). Рекомендація: внести зміни до Закону про хмарні технології та Закону про захист інформації, щоб дозволити міжнародним постачальникам послуг підтверджувати відповідність лише міжнародним стандартам інформаційної безпеки (наприклад, відповідність лише стандартам ISO/IEC 27001 та ISO/IEC 27018:2019). Прийняття всесвітньо визнаних стандартів, таких як ISO/IEC 27001 та ISO/IEC 27018:2019, оптимізує процеси відповідності також і для міжнародних CSP, що зробить Україну більш привабливим ринком для іноземних хмарних провайдерів. Таке узгодження також покращить	Відхилено. Стаття 8 Закону України “Про захист інформації в інформаційно-комунікаційних системах” передбачає, як застосування комплексної системи захисту інформації так і системи управління інформаційної безпеки, що врегульована міжнародним стандартом ISO/IEC 27018:2019. Яку із сертифікацій застосовувати є вибором Надавача хмарних послуг та вирівнює можливості українських та міжнародних надавачів хмарних послуг.

		взаємодію з глобальними хмарними службами, що принесе користь як місцевим підприємствам, так і державним установам. Крім того, міжнародні стандарти регулярно оновлюються для усунення нових загроз кібербезпеці, забезпечуючи більш надійний і сучасний захист, ніж потенційно застарілі місцеві стандарти. Прийнявши ці загальноприйняті норми, Україна продемонструвала б свою відданість найкращим світовим практикам хмарних обчислень і захисту даних, потенційно прискоривши свою цифрову трансформацію та інтеграцію в глобальну цифрову економіку.	
19.	До проекту постанови в цілому.	(iii) Забезпечення виконання місцевого законодавства України щодо угод про хмарні послуги Проблема: відповідно до Закону про хмарні технології (стаття 10, частина 3), договори про хмарні послуги з державними клієнтами повинні регулюватися законодавством України та вирішуватися в українських судах. Відповідні правила є недоцільними для роботи міжнародних постачальників послуг з українськими державними замовниками, оскільки міжнародні постачальники послуг зазвичай використовують власну уніфіковану перевірену типову угоду з усіма клієнтами в усьому світі, яка містить найкращі ринкові практики та договірні стандарти. Рекомендація: доповнити статтю 10 частини 3 Закону про хмарні технології застереженням, що дозволяє міжнародним провайдерам використовувати власні шаблони угод, які регулюються законодавством інших країн і вирішуються міжнародним арбітражем. Зобов'язання українським законодавством і судами укласти угоди про хмарні послуги з державними клієнтами створює значні юридичні та операційні проблеми для глобальних постачальників послуг, потенційно стримуючи їх від виходу на український ринок або розширення на ньому. Це обмеження обмежує доступ до передових хмарних технологій і послуг для українських державних установ, потенційно перешкоджаючи зусиллям з цифрової трансформації та конкурентним перевагам. Крім того, глобальні угоди міжнародних	Відхилено. Не є предметом регулювання проекту постанови. Зазначені пропозиції будуть враховані у подальшій роботі під час розробки інших нормативно-правових актів.

		провайдерів часто включають найкращі практики та надійні заходи безпеки, що приносить користь українським клієнтам. Дозвіл міжнародним провайдерам послуг використовувати свої встановлені шаблони договорів, які регулюються законодавством інших країн, приведе Україну до світової ділової практики.	
20.	До проекту постанови в цілому.	(iv) Дозвіл державним клієнтам використовувати хмару за межами України після закінчення воєнного стану Проблема: Закони України містять обмеження для державних установ щодо зберігання певних даних у хмарі за межами України. Ці обмеження призупиняються під час воєнного стану та певного проміжного періоду, але після цього відновляться. Такі обмеження обмежують доступ українських державних клієнтів до міжнародних CSP та стримують ініціативи щодо співпраці між ними навіть під час воєнного стану (багато установ не бажають зберігати дані за межами України, знаючи, що в майбутньому їм знадобиться перенести їх назад). У квітні 2024 року до Закону про хмари було внесено зміни, які обмежують вимогу щодо локалізації обробки даних державними установами лише даними, що становлять державну таємницю (скасовуючи попереднє обмеження щодо локалізації, що також стосується інформації внутрішнього використання та публічних реєстрів). Це крок до лібералізації української хмарної нормативно-правової бази. Однак існує ряд інших чинних правових актів, які все ще містять подібні обмеження, що перешкоджають можливості використання хмари за межами України Зняття обмежень щодо резидентності даних для державних установ в Україні значно розширить доступ до передових хмарних сервісів і сприятиме цифровій трансформації. Поточні обмеження, навіть якщо вони були призупинені під час воєнного стану, створюють невпевненість і небажання серед державних установ повною мірою використовувати міжнародні хмарні рішення. Дозволивши зберігання даних у регіоні ЄС чи НАТО, Україна може знайти баланс між	Відхилено. Не є предметом регулювання проекту постанови. Зазначені пропозиції може бути розцінено, як такі, що несуть шкоду національному суверенітету України.

		проблемами безпеки даних і потребою в технологічному прогресі. Такий підхід вирівняв би Україну з найкращими світовими практиками. Важливо відзначити, що CSP, які працюють у всьому світі, часто пропонують чудові рішення безпеки даних. Ці провайдери вкладають значні кошти в найсучасніші заходи безпеки, наймають глобальні команди експертів з кібербезпеки та постійно оновлюють свої системи, щоб протистояти новим загрозам. Їх масштаб дозволяє їм впроваджувати надійні протоколи безпеки, передові методи шифрування та багаторівневі механізми захисту. Дозволити державним установам скористатися цими розширеними заходами безпеки, а також економією за рахунок масштабу та передовими технологіями, які пропонують глобальні CSP, значно покращить захист даних, стимулюючи інновації. Усунення обмежень також оптимізує діяльність державних установ, усунувши потребу в майбутній міграції даних і зменшивши пов'язані з цим витрати та ризики. Крім того, це продемонструвало б відданість України цифровим інноваціям і міжнародній співпраці, потенційно прискоривши її інтеграцію в глобальну цифрову економіку. Застосовуючи більш відкритий підхід до зберігання даних, зберігаючи відповідні гарантії захисту державних таємниць, Україна може позиціонувати себе як далекоглядну націю, готову використовувати весь потенціал хмарних обчислень для покращення державних послуг та економічного зростання, водночас отримуючи вигоду від підвищеної безпеки, яку пропонують CSP. Рекомендація: Скасувати обмеження в усіх нормативно-правових актах, які забороняють державним замовникам зберігати дані (державну таємницю) за межами України навіть після припинення воєнного стану. Нижче наведено перелік правових актів і статей, які все ще містять обмеження:	
--	--	---	--

		• Закон України «Про публічні електронні реєстри» №. 1907-IX від 18.11.2021 (ст. 38); • Закон України Про захист інформації в інформаційно-комунікаційних системах № 80/94-ВР від 05.07.1994 р. (ст. 5); • Закон України «Про захист персональних даних» №. 2297-VI від 01.06.2010 (ч. 3 ст. 4); • Постанова Кабінету Міністрів України «Про деякі питання забезпечення функціонування державних інформаційних ресурсів» № 2007/2009. 1500 від 30 грудня 2022 року; • Постанова Кабінету Міністрів України «Про загальні вимоги до кіберзахисту об'єктів критичної інфраструктури» № 2007. 518 від 19 червня 2019 року (розділи 3, 6 та 49); • Постанова Кабінету Міністрів України «Про деякі питання забезпечення функціонування інформаційно-комунікаційних систем, систем електронного зв'язку, публічних електронних реєстрів в умовах воєнного стану» від 17.06.2017 р. 263 від 12.03.2022 (розділи 1 та 3).	
21.	До проекту постанови в цілому.	(v) Хмарна структура закупівель для державних клієнтів Проблема: державні клієнти повинні дотримуватися загальних процедур державних закупівель, які не підходять для хмарних служб. Наразі під час воєнного стану в Україні дію цих вимог призупинено. Проте через 90 днів після закінчення або скасування воєнного стану знову почнуть діяти стандартні правила публічних закупівель. Стандартні моделі закупівель не пристосовані до природи хмари і ускладнюють державним установам закупівлю хмарних послуг, які часто базуються на системі оплати за використання, а не на основі капітальних витрат.	Враховано частково. У пункті 2 проекту постанови слова “до 31 березня 2025 р.” замінено на слова “до 31 грудня 2025 р.” Зазначені пропозиції будуть враховані у подальшій роботі під час розробки інших нормативно-правових актів.

		Рекомендація: внести зміни до Закону України «Про публічні закупівлі» (його нова редакція знаходиться на розгляді в українському парламенті), щоб включити окремі положення щодо хмарних сервісів, дозволяючи більш тривалий термін і угоди з одним учасником. Внесення змін до Закону України «Про публічні закупівлі» щодо включення окремих положень щодо хмарних сервісів має вирішальне значення для модернізації ІТ-інфраструктури державного сектора. Поточні процедури закупівель, призначені в основному для традиційних товарів і послуг, погано підходять для динамічної природи хмарних обчислень. Хмарні сервіси часто працюють на основі гнучкої моделі, заснованої на споживанні, що суперечить жорсткому, орієнтованому на капітальні витрати підходу стандартних процесів закупівель. Запроваджуючи правила, пов'язані з хмарою, державні установи можуть ефективніше використовувати переваги хмарних обчислень, включаючи масштабованість, економічну ефективність і доступ до передових технологій. Бажано збільшити час, необхідний для впровадження необхідних змін. Довший період дозволить провести ретельні консультації із зацікавленими сторонами, включаючи постачальників хмарних послуг, ІТ-лідерів державного сектору та юридичних експертів. Цей розширений часовий проміжок забезпечить, щоб нові правила були комплексними, добре продуманими та відповідали як потребам державних установ, так і реаліям ринку хмарних послуг. Це також надасть достатньо часу державним установам для підготовки до нових моделей закупівель, оновлення своїх внутрішніх процесів і навчання персоналу відповідно.	
22.	До проекту постанови в цілому.	(vi) Класифікація даних Проблема: у нормативно-правових актах використовуються різні правові терміни та визначення під час опису типів даних (наприклад, «державні інформаційні ресурси», «інформація з обмеженим доступом», «державна таємниця», «інформація внутрішнього	Відхилено. Наведені терміни не є такими, що відносяться лише до даних та мають визначення відповідно до законодавства.

		користування», «державні реєстри», «публічні електронні реєстри»). Це призводить до відсутності ясності щодо того, які типи даних можна зберігати в хмарі/у хмарі за кордоном. Рекомендація: ввести чітку уніфіковану схему класифікації даних до Закону про хмару та Закону про захист інформації, щоб уточнити, які дані можна зберігати за межами України. Ця уніфікована система класифікації усуне двозначність і неузгодженість між різними правовими актами, забезпечуючи стандартизовану основу для обробки даних і рішень щодо зберігання. Чітка схема класифікації дозволить державним установам приймати обґрунтовані рішення щодо місць зберігання даних, оптимізуючи процеси відповідності та зменшуючи ризик ненавмисних порушень. Це також сприяло б більш ефективному впровадженню хмарних сервісів, усунувши невизначеності щодо вимог до зберігання даних. Крім того, уніфікована система класифікації покращить взаємодію між різними урядовими установами та системами, сприяючи кращому обміну даними та співпраці. Ця ясність також принесе користь CSP, дозволяючи їм адаптувати свої пропозиції для більш ефективного виконання конкретних вимог класифікації даних.	Чинним законодавством визначено класифікацію даних та відмінності між ними, зокрема у статтях 10-21 Розділу II Закону України “Про інформацію”.
23.	Пункт 3 проекту Порядку надання хмарних послуг: “3. ... Строк дії договору про надання хмарних послуг та/ або послуг центру обробки даних (далі - договір) повинен визначатись з урахуванням строку дії документу про	Maxim Ageyev Така вимога порушує логіку сертифікації та не відповідає існуючій практиці. З даного формулювання виходить, що, якщо документ про відповідність завершує свою дію в грудні, а договір підписується в січні того ж року, то надавач хмарних послуг повинен почати переатестацію/ресертифікацію на рік раніше, ніж це передбачають правила отримання документу про відповідність. Пропонується:	Відхилено. Запропонована пропозиція суперечить інтересам користувача хмарних послуг. Норма про розірвання, передбачена у пункті 37 проекту Типового договору.

	відповідність та не бути більшим строку дії такого документу.”	Абзац необхідно видалити, так як в типовому договорі на випадок припинення або скасування документу про відповідність передбачена можливість дострокового розірвання Договору (п.37)	
24.	Пункт 4 Порядку надання: “4. Під час аналізу ринку надавачів з метою порівняння їх послуг, зокрема щодо управління інформаційною безпекою, управління безперервністю надання послуг, управління якістю, впливу на довкілля...”	Пропонується: Перелік вимог має бути чітко прив’язаний до певних стандартів. Це має бути зроблено на базі існуючих ринкових практик. Наприклад, стандарт управління якістю ISO9001 не має широкого розповсюдження на ринку хмарних послуг. Стандарти інформаційної безпеки також можуть мати міжнародний або більш локальний характер (наприклад, тільки на території США або ЄС). Нечіткість формулювань дає можливість неринкових маніпуляцій	Відхилено. Користувач повинен використовувати інформацію, визначену у Переліку та електронному каталозі.
25.	Пункт 8 проекту Порядку надання: “8. ... Електронні інформаційні ресурси передаються до нового надавача у повному обсязі. Витрати на проведення робіт, пов’язаних з передачею електронних інформаційних ресурсів несе новий надавач ”.	Пропонується: Вимога про витрати на міграцію виглядає як обов’язкова та безальтернативна. При цьому ніяк не розтлумачено природу передачу електронних носіїв. Вимогу треба або прибрати (наприклад, зробити пунктом договору, який погоджують надавач та користувач), або детально прописати процедуру переносу й розрахунку ціни міграції. Наприклад, для переносу прикладного ландшафту треба використовувати адміністративні права, які має тільки користувач. Тож надавач не може цього зробити by design.	Відхилено. Відсутні підстави фінансово навантажувати користувача хмарних послуг, який мігрує за результатами тендеру.
26.	Підпункт 3 пункту 12 проекту Порядку	Пропонується: Вимога не відповідає існуючим практикам.	Враховано. У підпункті 3 пункту 12

	підтвердження відповідності: “12. Моніторинг, аудит та випробування забезпечується: ... 3) регулярним (не менш ніж один раз на місяць) проведенням випробувань (тестів) для виявлення загальновідомих вразливостей системних компонентів, які використовуються для надання послуг;”	Наприклад, зараз самий вибагливий це стандарт PCIDSS і він каже про один раз на квартал	проекту Порядку підтвердження відповідності слова “не менш ніж один раз на місяць” замінено словами “не менш ніж один раз на квартал”.
27.	Проектом акта передбачається затвердити Типовий договір про надання хмарних послуг та/або послуг центру обробки даних публічному користувачу та об’єкту критичної інформаційної інфраструктури (далі - проект Типового договору).	Проект договору не містить можливості зміни переліку та кількості послуг в рамках суми договору (хоча в п.19 прописано, що оплата відбувається за фактично надані Послуги і в п.2 зазначено, що ціна договору складається з вартості наданих послуг). Пропонується: Необхідно додати пункт: «Перелік та обсяг хмарних ресурсів, що надаються за цим Договором, визначається згідно замовлень на Послуги, якщо інше не передбачено умовами Договору. Зміна переліку та/або обсягу хмарних ресурсів здійснюється шляхом надання Замовником нового замовлення на Послуги»	Враховано редакційно. Пункт 25 проекту Типового договору доповнено підпунктом 4 у такій редакції: “Користувач має право: ... 4) змінювати обсяг послуг, що надаватимуться у відповідний звітний період шляхом укладення додаткової угоди.”

28.	Пункт 6 проекту Типового договору: “6. Користувач в строк _____ робочих днів після підписання цього Договору передає дані, операційні та інформаційні системи (за наявності) Надавачу для забезпечення надання Послуг та виконання умов цього Договору”	Пропонується: «Користувач в строк _____ робочих днів після підписання цього Договору передає дані (у об'ємі та форматі, який відповідає виду хмарних послуг відповідно до Закону України «Про хмарні послуги»), операційні та інформаційні системи (за наявності) Надавачу для забезпечення надання Послуг та виконання умов цього Договору...» Формулювання без такого уточнення означає, що надавач буде мати доступ безпосередньо до даних Користувача (і як результат змінювати ці дані, зчитувати їх)	Відхилено. Формат даних визначено пунктами 7, 8 проекту Порядку надання та технічними умовами договору.
29.	Пункт 41 проекту Типового договору: “41. У разі відсутності пропозиції (повідомлення) однієї зі Сторін про припинення або зміни до цього Договору за _____ місяці до закінчення строку дії цього Договору він вважається продовженням на той самий строк і на тих самих умовах, які були передбачені цим Договором.”	Дивний пункт. Я так розумію, що державні органи закуповують послуги через тендер? І в тендерних умовах зазначається строк на який може бути заключений договір і автоматичному пролонгуванню такі договори не підлягають. Пропонується: Такий пункт неприпустимий в договорах, які підписуються за результатом проведеної закупівлі.	Враховано. Пункт 41 Типового договору виключено.
30.	Проектом акта передбачається	Пропонується:	Відхилено. Проектом не вимагається

	затвердити додаток до Порядку формування та використання електронних каталогів хмарних послуг та/або послуг центру обробки даних “Структура електронних каталогів” (далі- проект Структури каталогів). Пункт 17 проекту Структури каталогів: “17. Порядок захисту даних (загальна інформація щодо заходів захисту, у тому числі криптографічного захисту даних при передачі та зберіганні, застосованих протоколів, алгоритмів) <i>Посилання на вебсторінку надавача з більш детальною інформацією про захист даних”.</i>	Детальний опис протоколів, алгоритмів захисту тощо є конфіденційною інформацією та не підлягає розголошенню	детального опису, лише загальна інформація щодо заходів захисту
31.	Пункт 21 проекту Структури електронних каталогів: “21. Відповідність стандартам, вимогам	Приведені формулювання дають можливість використовувати виключно національні сертифікати. Пропонується: краще, щоб цей пункт мав таку ж саму редакцію, як в п. 14 документу «Порядок та Вимоги до надавачів послуг хмари», а саме:	Враховано редакційно. Пункт 21 проекту Структури електронних каталогів викладено у такій редакції:

	законодавства, які застосовуються до вказаних у Каталогі послуг (стандарти ДСТУ EN ISO/IEC 27001:2022 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги” (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT), ДСТУ EN ISO/IEC 27017:2022 “Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг” (EN ISO/IEC 27017:2021, IDT; ISO/IEC 27017:2015, IDT), ДСТУ EN ISO/IEC 27018:2022 “Інформаційні технології. Методи захисту. Кодекс	«відповідність міжнародному стандарту ISO/IEC 27001 або національному стандарту іноземної країни, прийнятому відповідно до міжнародного стандарту ISO/IEC 27001, або ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27018:2019 «Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII» (ISO/IEC 27018:2019, IDT).»	“21. Відповідність міжнародному стандарту ISO/IEC 27001 або національному стандарту іноземної країни, прийнятому відповідно до міжнародного стандарту ISO/IEC 27001, або ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27018:2019 «Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII» (ISO/IEC 27018:2019, IDT).”
--	--	--	--

	усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII” (EN ISO/IEC 27018:2020, IDT; ISO/IEC 27018:2019, IDT), наявність чинних сертифікатів, аудиторських звітів). <i>Посилання на вебсторінку надавача з більш детальною інформацією про відповідність стандартам та законодавству. ”</i>		
32.	До проекту постанови в цілому.	Marcin Krasuski Ми хотіли б висловити серйозну стурбованість щодо доцільності завершення роботи TAB та імплементації її висновків до української законодавчої бази до кінця березня 2025 року. Запропонований проект буде прийнято до впровадження змін, є висока ймовірність того, що з 1 квітня Google та іншим неукраїнським хмарним провайдером буде заборонено надавати послуги значна частина державного сектора України. Це призвело б до раптового припинення існуючої співпраці з потенційно серйозними наслідками. Ми наполегливо закликаємо переглянути запропонований графік і графік впровадження, щоб уникнути такого руйнівного результату. Тому ми рекомендуємо відкласти прийняття даної постанови до вирішення законодавчих	Враховано. У пункті 2 проекту постанови слова “до 31 березня 2025 р.” замінено на слова “до 31 грудня 2025 р.”

		питань. Після цих змін статут слід переглянути, щоб забезпечити повну відповідність оновленій структурі.	
33.	До проекту постанови в цілому.	Американська торгівельна палата в Україні Експерти компаній-членів Палати ознайомилися із вищезгаданим Проектом та дійшли висновку, що він не узгоджується із існуючими рамками співпраці компаній-членів з Мінцифри та Урядом України загалом. Безумовно, впровадження запропонованого нормативного акта в його нинішньому вигляді не тільки суттєво ускладнить впровадження хмарних технологій для українських та міжнародних постачальників хмарних послуг, а й негативно вплине на поточну та подальшу співпрацю з міжнародними постачальниками хмарних послуг. Окрім того, ухвалення запропонованого Проекту, ймовірно, призведе до зупинення надання хмарних послуг і продуктів кібербезпеки, включно з тими, які зараз надаються державним установам безкоштовно. Більше того, стратегія цифровізації України, включно зі сферою кібербезпеки, зазнає негативного впливу в майбутньому. У разі необхідності, експерти компаній-членів Палати готові долучитися до обговорення Проекту з представниками Мінцифри та надати необхідну експертну підтримку. Наразі просимо відкласти прийняття Проекту до узгодження всіх питань, які були донесені до Мінцифри в попередніх листах Палати: № 22–74 від 21 січня 2022 року; № 23–601 від 14 грудня 2023 року та № 24–201 від 26 квітня 2024 року.	Враховано редакційно. У пункті 2 проекту постанови слова “до 31 березня 2025 р.” замінено на слова “до 31 грудня 2025 р.”
34.	До проекту Порядку надання в цілому.	Товариство з обмеженою відповідальністю «ГІГЛАУД» 1. Принципова пропозиція – розмежувати порядок та умови надання хмарних послуг та послуг центру обробки даних та хмарної	Відхилено. Зазначені пропозиції будуть враховані у подальшій роботі під час розробки інших нормативно-правових актів.

		інфраструктури як такі, до яких застосовуються різні вимоги та умови надання послуг.	
35.	Пункт 3 проекту Порядку надання: “3. Під час вибору хмарних послуг та/або послуг центру обробки даних та хмарної інфраструктури публічний користувач хмарних послуг або користувач хмарних послуг та/або послуг центру обробки даних, що є власником (держателем, розпорядником) електронних інформаційних ресурсів (далі - користувач), враховує документ про відповідність, виданий акредитованим органом з оцінки відповідності в сфері електронних комунікацій, щодо відповідної хмарної послуги та/ або послуги центру обробки даних, який є достатнім документальним підтвердженням щодо	2. Підтвердження сертифікації (наприклад ISO) раніше закінчення попереднього строку не передбачено умовами сертифікації (том що оцінюється виконання умов сертифікації протягом всього строку дії сертифікату). Тобто буде ситуація у всіх надавачів, коли попередній сертифікат вже закінчився, а нового на підтвердження ресертифікації ще не видали (в процесі отримання). Останнє речення п. 3 видалити.	Відхилено. Запропонована пропозиція суперечить інтересам користувача хмарних послуг.

	управління інформаційною безпекою, неперервністю, безпеки мережевих та інформаційних систем надавачів хмарних послуг та/або послуг центру обробки даних (далі - надавач). Строк дії договору про надання хмарних послуг та/ або послуг центру обробки даних (далі - договір) повинен визначатись з урахуванням строку дії документу про відповідність та не бути більшим строку дії такого документу.”		
36.	Пункт 8 проекту Порядку надання: “8. Передача даних від користувача, а також від надавача до їх користувача, повинна відбуватись у структурованому вигляді, що дозволяє їх належне використання, обробку та інтеграцію з	3. Передача даних у структурованому вигляді не передбачена суттю таких послуг центру обробки даних як - розміщення обладнання у центрі обробки даних, включаючи надання у користування окремих приміщень для розміщення обладнання; - надання у користування технічних засобів, розміщених у центрі обробки даних; - кіберзахисту. Для цих послуг – розміщується обладнання, а не дані. Надавач послуг не має доступу до даних... Пропонується така редакція:	Відхилено. Зазначені пропозиції будуть враховані у подальшій роботі під час розробки інших нормативно-правових актів.

	іншими системами. Дані мають передаватись у форматах, що забезпечують можливість зчитування, збереження логічної структури даних та їх інтерпретування при обробці та дозволяють автоматизовану обробку даних без застосування додаткових засобів щодо їх конвертації. Детальні умови передачі даних щодо їх структурування та форматів визначаються договором. Порядок, вимоги до процесів, технічні вимоги, строки та підстави передачі електронних інформаційних ресурсів від одного надавача до іншого надавача, в тому числі, у випадках залучення надавачем іншого надавача, або у разі переходу користувача до іншого надавача,	“8. Передача даних від користувача, а також від надавача до їх користувача, повинна відбуватись у структурованому вигляді (для хмарних послуг та послуг центру обробки даних, де передбачається сама передача даних), що дозволяє їх належне використання, обробку та інтеграцію з іншими системами. Дані мають передаватись у форматах, що забезпечують можливість зчитування, збереження логічної структури даних та їх інтерпретування при обробці та дозволяють автоматизовану обробку даних без застосування додаткових засобів щодо їх конвертації. Детальні умови передачі даних щодо їх структурування та форматів визначаються договором. Порядок, вимоги до процесів, технічні вимоги, строки та підстави передачі електронних інформаційних ресурсів від одного надавача до іншого надавача, в тому числі, у випадках залучення надавачем іншого надавача, або у разі переходу користувача до іншого надавача, зокрема, за результатами проведення процедур закупівель, передбачаються в договорі. Електронні інформаційні ресурси передаються до нового надавача у повному обсязі. Витрати на проведення робіт, пов'язаних з передачею електронних інформаційних ресурсів несе новий надавач.”	
--	--	--	--

	зокрема, за результатами проведення процедур закупівель, передбачаються в договорі. Електронні інформаційні ресурси передаються до нового надавача у повному обсязі. Витрати на проведення робіт, пов'язаних з передачею електронних інформаційних ресурсів несе новий надавач. У разі переходу користувача до іншого надавача такий користувач не пізніше ніж за один календарний місяць до запланованої дати припинення використання хмарних послуг та/або послуг центру обробки даних повідомляє відповідного надавача про необхідність, умови та порядок передачі даних. У разі відмови користувача від		
--	---	--	--

	використання хмарних послуг та/або послуг центрів обробки даних, такий користувач не пізніше ніж за один календарний місяць до запланованої дати припинення використання хмарних послуг повідомляє відповідного надавача про рішення, умови та порядок передачі, а також порядок видалення даних. У всіх випадках передача електронних інформаційних ресурсів повинна здійснюватись з дотриманням вимог законодавства у сфері захисту інформації та кібербезпеки. У разі переходу користувача до іншого надавача або відмови від хмарних послуг, такому користувачу у чіткій та доступній формі повинна надаватися інформація щодо: процесів в обсязі, необхідному для		
--	--	--	--

	попереднього розрахунку вартості робіт для передачі даних та припинення обробки; технічних вимог в обсязі, достатньому для оцінки сумісності при переході до іншого надавача або для можливості збереження даних у разі відмови від хмарних послуг; строків, за який має бути проведено перехід до іншого надавача або передачі та порядку видалення даних та суми платежів в тому числі додаткових, що виникають.”		
37.	Пункт 16 проекту Порядку підтвердження відповідності: “16. Відповідність вимогам до надавача підтверджується: 1) документом про відповідність, виданим органом з оцінки відповідності, та/або документом з	П. 16 Порядку не відповідає в повній мірі ч. 3 ст. 8 Закону України «Про хмарні послуги», яка визначає окремо вимоги до надавачів хмарних послуг та до надавачів послуг центру обробки даних: <i>«4) засвідчені в установленому порядку копії документів, що підтверджують право власності або право користування засобами, що використовуються при наданні хмарних послуг»;</i> В той же час, пп. 3 п. 16 Порядку розширені і для надання послуг центру обробки даних. Пп. 5 п. 16 Порядку дублює рп. 6 ч. 3 ст. 8 закону України «Про хмарні послуги», в той же час, цей Порядок і є вимогами до надавачів хмарних послуг та/або послуг центру обробки даних, затверджені Кабінетом	Враховано редакційно. Стаття 8 Закону України «Про хмарні послуги» визначає вимоги до надавача хмарних послуг та/або послуг центру обробки даних та не передбачає необхідності їх розділення. Норми, передбачені частиною четвертою статті 8 Закону України «Про хмарні послуги»

	підтвердження відповідності, комплексної системи захисту інформації за результатами державної експертизи у сфері технічного захисту інформації; 2) документами, що визначають порядок обробки персональних даних чи політики, якими регламентовано дотримання конфіденційності обробки персональних даних; 3) документами, що підтверджують право власності або право користування засобами, що використовуються при наданні хмарних послуг та/або послуг центру обробки даних у разі відсутності такої інформації в публічних електронних реєстрах, інформаційно-комунікаційних системах;	Міністрів України. Тобто виходить що цей Порядок посилається на документ, який сам же і має визначити, але Порядок його не визначає! Що це за документ – потрібно уточнити/конкретизувати додатково в цьому Порядку! «орган з оцінки відповідності у сфері електронних комунікацій» пп. 5 п. 16 Порядку – законодавством окремо не визначений. Порядок має конкретизувати який саме орган має видавати такий документ і що це за документ має бути. Не врахована вимога ч. 4 ст. 8 закону України «Про хмарні послуги» - право на ПЗ для надання хмарних послуг. Пропонується така редакція: “16. Відповідність вимогам до надавача підтверджується: 1) документом про відповідність, виданим органом з оцінки відповідності, та/або документом з підтвердження відповідності, комплексної системи захисту інформації за результатами державної експертизи у сфері технічного захисту інформації; 2) документами, що визначають порядок обробки персональних даних чи політики, якими регламентовано дотримання конфіденційності обробки персональних даних; 3) документами, що підтверджують право власності або право користування засобами, що використовуються при наданні хмарних послуг у разі відсутності такої інформації в публічних електронних реєстрах, інформаційно-комунікаційних системах; 4) документами, що підтверджують право власності або право користування приміщеннями, що використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання хмарних послуг для надавачів послуг центру обробки даних; 5) документом про відповідність юридичних осіб, фізичних осіб – підприємців, які мають намір надавати хмарні послуги та/або послуги центру обробки даних, цьому Порядку, який видається регулятором комунікаційних послуг або іншим уповноваженим органом з оцінки відповідності. 6) Надавачі хмарних послуг, крім надавачів інфраструктури як послуги, додатково подають засвідчені в установленому порядку	викладено редакційно у підпункті 3 пункту 16 проекту Порядку підтвердження відповідності.
--	--	---	--

	4) документами, що підтверджують право власності або право користування приміщеннями, що використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання хмарних послуг для надавачів послуг центру обробки даних; 5) документом про відповідність, виданим органом з оцінки відповідності у сфері електронних комунікацій, що підтверджує відповідність юридичних осіб, фізичних осіб – підприємців, які мають намір надавати хмарні послуги та/або послуги центру обробки даних, цим Порядку та вимогам.”	копії документів, що підтверджують право користування або розповсюдження апаратного або програмного забезпечення, що буде застосовуватися при наданні хмарних послуг.	
38.	До проекту Типового договору в цілому.	Принципова пропозиція – розмежувати істотні умови з надання хмарних послуг та істотні умови з надання послуг центру обробки	Відхилено. Зазначені пропозиції будуть

		даних та хмарної інфраструктури як такі, до яких застосовуються різні вимоги та умови надання послуг.	враховані у подальшій роботі під час розробки інших нормативно-правових актів.
39.	Пункт 3 проекту Типового договору: “3. Надавач надає Користувачу доступ до хмарних ресурсів після отримання від користувача Переліку авторизованих осіб, форма якого визначена у додатку 3 до Договору.	Умова «доступ до хмарних ресурсів» не застосовна до ресурсів ЦОД. Пропонується така редакція: “3. Надавач надає Користувачу доступ до хмарних ресурсів або ресурсів центру обробки даних після отримання від користувача Переліку авторизованих осіб, форма якого визначена у додатку 3 до Договору. У разі зміни авторизованих осіб, Користувач надає Надавачу оновлення до Переліку авторизованих осіб не пізніше наступного робочого дня з дати зміни авторизованих осіб.”	Враховано.
40.	Пункт 4 проекту Типового договору: 4. Надавач надає Користувачу дані для автентифікації для доступу до хмарних ресурсів.	Пропонується така редакція: “4. Надавач надає Користувачу дані для автентифікації для доступу до хмарних ресурсів або ресурсів центру обробки даних. ”	Враховано.
41.	Пункт 5 проекту Типового договору: 5. Авторизовані особи використовують надані дані для автентифікації для доступу до хмарних ресурсів, що обробляються під час виконання Договору особисто. Авторизовані	Пропонується така редакція: “5. Авторизовані особи використовують надані дані для автентифікації для доступу до хмарних ресурсів, що обробляються під час виконання Договору особисто або ресурсів центру обробки даних. Авторизовані особи не можуть передавати дані для автентифікації третім особам.”	Враховано.

	особи не можуть передавати дані для автентифікації третім особам.		
42.	Пункт 7 проекту Типового договору: 7. Порядок та періодичність здійснення резервного копіювання інформації Надавачем, періодичність перевірки резервних копій, термін їх зберігання визначаються у Технічних вимогах.	Для таких послуг ЦОД як: «- розміщення обладнання у центрі обробки даних, включаючи надання у користування окремих приміщень для розміщення обладнання; - надання у користування технічних засобів, розміщених у центрі обробки даних;» Резервне копіювання здійснюється самим Користувачем, Надавач за загальним правилом не має взагалі доступу до даних, яка розміщена на обладнанні Користувача в ЦОД. Пропонується така редакція: “7. Порядок та періодичність здійснення резервного копіювання інформації Надавачем, періодичність перевірки резервних копій, термін їх зберігання визначаються у Технічних вимогах у випадках, коли це застосовано до Послуг ”	Відхилено. Редакція пункту 7 проекту Типового договору, що стосується Надавача викладена досить загально та охоплює випадки, коли це застосовано до Послуг.
43.	Пункт 10 проекту Типового договору: 10. Надавач забезпечує захист даних (у тому числі персональних) при наданні послуг, у тому числі від несанкціонованих дій (внутрішніх та зовнішніх загроз, інцидентів кібербезпеки, сеп кібератак), відповідно до політик безпеки	Обсяги захисту для хмарних послуг та послуг ЦОД істотно відрізняються. Пропонується така редакція: “10. Надавач у визначених цим Договором обсягах забезпечує захист даних (у тому числі персональних) при наданні послуг, у тому числі від несанкціонованих дій (внутрішніх та зовнішніх загроз, інцидентів кібербезпеки, кібератак), відповідно до політик безпеки впроваджених відповідно побудованих системи управління інформаційної безпеки та/або комплексної системи захисту інформації на хмарні ресурси та документів, що визначають порядок обробки персональних даних.”	Відхилено. Норми щодо захисту даних (у тому числі персональних) визначені на законодавчому рівні, а не лише в обсягах, визначених договором.

	впроваджених відповідно побудованих системи управління інформаційної безпеки та/або комплексної системи захисту інформації на хмарні ресурси та документів, що визначають порядок обробки персональних даних.		
44.	Пункт 26 проекту Типового договору: 26. Надавач зобов'язаний: 4) у разі припинення Договору невідкладно, але в будь-якому випадку не пізніше двох робочих днів з дати завершення передачі даних (інформації), у тому числі їх резервних копій, що були накопичені, створені у процесі виконання Договору, видалити всі дані Користувача, що оброблялись, зберігались або накопичувались на	Для таких послуг ЦОД як: «- розміщення обладнання у центрі обробки даних, включаючи надання у користування окремих приміщень для розміщення обладнання; - надання у користування технічних засобів, розміщених у центрі обробки даних;» Резервне копіювання здійснюється самим Користувачем, Надавач за загальним правилом не має взагалі доступу до даних, яка розміщена на обладнанні Користувача в ЦОД. Формулювання в редакції Типового договору буквально означає видалення всіх даних Користувача, тобто і про Користувача, тоді Надавач не може використовувати дані про Користувача в договорі, акті, податкових накладних. Пропонується така редакція: “26. Надавач зобов'язаний: 4) коли це застосовно до Послуг – у разі припинення Договору невідкладно, але в будь-якому випадку не пізніше двох робочих днів з дати завершення передачі даних (інформації), у тому числі їх резервних копій, що були накопичені, створені у процесі виконання Договору, видалити всі дані Користувача, що оброблялись, зберігались або накопичувались на будь-яких інформаційних, комунікаційних, програмних або апаратних ресурсах Надавача та надати Користувачу	Відхилено. Не є предметом регулювання проекту постанови. Зазначені пропозиції будуть враховані у подальшій роботі під час розробки інших нормативно-правових актів.

	будь-яких інформаційних, комунікаційних, програмних або апаратних ресурсах Надавача та надати Користувачу письмове підтвердження щодо видалення (знищення) даних Користувача;	письмове підтвердження щодо видалення (знищення) даних Користувача (крім тих, які Надавач має зберігати для виконання вимог законодавства)”	
45.	Пункт 41 проекту Типового договору: “41. У разі відсутності пропозиції (повідомлення) однієї зі Сторін про припинення або зміни до цього Договору за _____ місяці до закінчення строку дії цього Договору він вважається продовженим на той самий строк і на тих самих умовах, які були передбачені цим Договором.”	Не відповідає практиці публічних закупівель за ЗУ «Про публічні закупівлі». Або треба прописати цю умову як особливість закупівель через електронний каталог. Пропонується виключити.	Враховано. Пункт 41 Типового договору виключено.
46.	Пункт 16 проекту Структури каталогів: “16. Місце розташування хмарних ресурсів, центру	Потрібно уточнити можливість зазначення загального уточнення місця розташування хмарних ресурсів, ЦОД (країна/місто) як об’єктів критичної інфраструктури, об’єктів інформаційної критичної інфраструктури; Пропонується така редакція:	Відхилено. Редакція пункту 16 проекту Типового договору є досить загальною та передбачає зазначення країни, місця

	обробки даних, в тому числі, зовнішніх постачальників, за допомогою яких надаються послуги (країна, можливість вибору місця розташування користувачем та здійснення контролю за місцем розташування) <i>Посилання на веб-сторінку надавача з більш детальною інформацією про місце розташування хмарних ресурсів, центру обробки даних, в тому числі, зовнішніх постачальників та можливість контролю”</i>	“16. Місце розташування хмарних ресурсів, центру обробки даних, в тому числі, зовнішніх постачальників, за допомогою яких надаються послуги (деталізація до рівня країна, місто, можливість вибору місця розташування користувачем та здійснення контролю за місцем розташування) <i>Посилання на веб-сторінку надавача з більш детальною інформацією про місце розташування хмарних ресурсів, центру обробки даних, в тому числі, зовнішніх постачальників та можливість контролю”</i>	розташування).
47.	Підпункт 3 пункту 12 проекту Порядку підтвердження відповідності: “12.Моніторинг, аудит та випробування забезпечується: ... 3) регулярним (не менш ніж один раз на місяць) проведенням	Асоціація «Телас» Практика підтримання системи в працездатному стані показує, що технічне втручання в систему щомісяця може призвести до можливих збоїв в роботі самої системи або порушення функціонування її цілісності. Пропонується така редакція: “3) регулярним (не менш ніж один раз на півроку) проведенням випробувань(тестів) для виявлення загальновідомих вразливостей системних компонентів, які використовуються для надання послуг;”	Враховано редакційно. У підпункті 3 пункту 12 проекту Порядку підтвердження відповідності слова “не менш ніж один раз на місяць” замінено словами “не менш ніж один раз на квартал”.

	випробувань (тестів) для виявлення загальновідомих вразливостей системних компонентів, які використовуються для надання послуг;”		
48.	До Порядку формування та використання електронних каталогів хмарних послуг та/або послуг центру обробки даних (далі - проект Порядку електронних каталогів) в цілому.	“8. На період дії воєнного стану в Україні, введеного Указом Президента України "Про введення воєнного стану в Україні" від 24 лютого 2022 року № 64/2022, затвердженим Законом України "Про затвердження Указу Президента України "Про введення воєнного стану в Україні" від 24 лютого 2022 року № 2102-ІХ, надавач забезпечує доступ до електронного каталогу виключно на запит публічного користувачу хмарних послуг або користувача хмарних послуг та/ або послуг центру обробки даних, що є власником (держателем, розпорядником) державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом та об'єктів критичної інформаційної інфраструктури.” Вважаємо, що така чутлива та важлива інформація не може бути у відкритому та публічному доступі враховуючи заходи безпеки.	Відхилено. Норми Закону України “Про хмарні послуги” не передбачають встановлення обмежень до такої інформації.
49.	Пункт 5 проекту Структури каталогів: “5. Вид хмарних послуг та/або послуг центру обробки даних відповідно до Закону України «Про хмарні послуги»: 1) інфраструктура як послуга;	Термін «безпека як послуга» за визначенням, що наведене у ч. 2 ст. 3 ЗУ «Про хмарні послуги», включає в себе термін «кіберзахист». Пропонується така редакція: “5. Вид хмарних послуг та/або послуг центру обробки даних відповідно до Закону України «Про хмарні послуги»: 1) інфраструктура як послуга; 2) платформа як послуга; 3) програмне забезпечення як послуга; 4) безпека як послуга; 5) інші послуги, що відповідають визначенню хмарних послуг;	Відхилено. Відповідно до частини четвертої статті 3 Закону України “Про хмарні послуги” до послуг центру обробки даних належать послуги з кіберзахисту.

	2) платформа як послуга; 3) програмне забезпечення як послуга; 4) безпека як послуга; 5) інші послуги, що відповідають визначенню хмарних послуг; 6) технічне адміністрування інформаційних (автоматизованих), електронних комунікаційних мереж та інформаційно-комунікаційних систем; 7) технічна підтримка користувача хмарних послуг та/або послуг центру обробки даних (далі - користувач); 8) розміщення обладнання у центрі обробки даних, включаючи надання у користування окремих приміщень для розміщення обладнання; 9) надання у користування технічних засобів,	6) технічне адміністрування інформаційних (автоматизованих), електронних комунікаційних мереж та інформаційно-комунікаційних систем; 7) технічна підтримка користувача хмарних послуг та/або послуг центру обробки даних (далі - користувач); 8) розміщення обладнання у центрі обробки даних, включаючи надання у користування окремих приміщень для розміщення обладнання; 9) надання у користування технічних засобів, розміщених у центрі обробки даних.”	
--	--	---	--

	розміщених у центрі обробки даних; 10) кіберзахист.”		
50.	Пункт 16 проекту Структури каталогів: “16. Місце розташування хмарних ресурсів, центру обробки даних, в тому числі, зовнішніх постачальників, за допомогою яких надаються послуги (країна, можливість вибору місця розташування користувачем та здійснення контролю за місцем розташування) <i>Посилання на веб-сторінку надавача з більш детальною інформацією про місце розташування хмарних ресурсів, центру обробки даних, в тому числі, зовнішніх постачальників та можливість контролю”</i>	Виключити. Ця інформація є дуже чутливою щоб виноситись на загал. Її розголошення може нанести шкоду постачальнику послуг та сприяти кіберзагрозам та/або фізичному знищенню за рахунок ракетно-дронових атак рф. Пропонуємо або виключити цей пункт або виділити вищевказану інформацію в окрему категорію, до якої матимуть доступ лише вповноважені представники держави та замовників послуг.	Відхилено. Редакція пункту 16 проекту Типового договору є досить загальною та передбачає зазначення країни, місця розташування.
51.	Пункт 19 проекту Структури каталогів:	Виключити.	Відхилено. Норми Закону України “Про

	“19. Здійснення повідомлень про інциденти (політики щодо повідомлення користувача послуг про інциденти безпеки, заплановані та позапланові експлуатаційні роботи, що можуть вплинути на рівень якості послуг). Посилання на вебсторінку надавача п з більш детальною інформацією про підтримку користувачів.”	Ця інформація є дуже чутливою щоб виноситись на загал. Її розголошення може нанести шкоду постачальнику послуг та сприяти кіберзагрозам та/або фізичному знищенню за рахунок ракетно-дронових атак рф. Пропонуємо або виключити цей пункт або виділити вищевказану інформацію в окрему категорію, до якої матимуть доступ лише вповноважені представники держави та замовників послуг.	хмарні послуги” не передбачають встановлення обмежень до такої інформації.
52.	Пункт 2 проекту Типового договору: “2. Ціна цього Договору складається із загальної вартості Послуг, наданих протягом строку дії Договору, і становить _____ грн., у тому числі ПДВ (якщо застосовується) – _____ грн.”	Не вбачається зрозумілим, яким чином можна дізнатись реально визначену суму, оскільки склад послуг може впродовж строку їх надання змінюватись.	Враховано редакційно. Пункт 25 проекту Типового договору доповнено підпунктом 4 такого змісту: “25. Користувач має право: ... 4) змінювати обсяг послуг, що надаватимуться у відповідний звітний період шляхом укладення додаткової угоди”.

53.	Пункт 18 проекту Типового договору: “18. Надавач має повідомити Користувача про відновлення доступності Послуг. Користувач має підтвердити відновлення доступності Послуг. У разі якщо Користувач підтвердив відновлення Послуг період недоступності Послуг вважається завершеним.”	Потребує доопрацювання розробником. Не повним виглядає алгоритм дій сторін за цим пунктом в частині відхилення рівня надання послуг, а також моменту з якого вважається, що послуга недоступна. Не зрозуміло, що має робити надавач, якщо користувач не підтвердив відновлення послуг.	Враховано. Пункт 18 проекту Типового договору викладено у такій редакції: “18. Надавач має повідомити Користувача про відновлення доступності Послуг. Користувач має підтвердити відновлення доступності Послуг не пізніше 12 годин з моменту такого відновлення. У разі якщо Користувач підтвердив відновлення Послуг період недоступності Послуг вважається завершеним”.
54.	Пункт 19 проекту Типового договору: “19. Плата за надані Послуги здійснюється Користувачем у безготівковій формі шляхом перерахування грошових коштів в національній валюті України на розрахунковий рахунок Надавача, визначений в цьому Договорі, протягом _____ банківських днів з дати	Є невідповідність у порядку оплати, оскільки в пункті 19 проекту Типового договору передбачено, що оплата здійснюється після підписання акту, а в пункті 21 зазначається, що після завершення періоду оплати надсилається акт.	Враховано редакційно. Пункт 21 проекту Типового договору викладено у такій редакції: “21. Не пізніше _____ робочих днів з дня завершення періоду надання Послуг Надавач передає Користувачу підписаний ним Акт приймання-передачі наданих Послуг. Користувач, у випадку відсутності зауважень до наданих Послуг, підписує зазначений Акт протягом _____ робочих днів з дати

	підписання Сторонами Акта приймання-передачі наданих Послуг за фактично надані Послуги.”		його отримання.”
55.	Пункт 24 проекту Типового договору: “Користувач звільняється від відповідальності за прострочення розрахунків за цим Договором у разі неналежного фінансування та/або відсутності фінансування з державного бюджету та/або нездійснення відповідних платежів органами Державної казначейської служби України відповідно до постанови Кабінету Міністрів України від 9 червня 2021 року № 590 “Про затвердження Порядку виконання повноважень Державною казначейською службою в особливому режимі в умовах	Виключити. Це може створити постійну дебіторську заборгованість з боку держави, без жодної відповідальності у вигляді пені. Держава має планувати бюджет на наступний рік та закладати кошти на оплату послуг.	Відхилено. Дана пропозиція суперечить інтересам користувача хмарних послуг.

	воєнного стану” (Офіційний вісник України, 2021 р., № 48, ст. 2974)”. 		
56.	Підпункт 5 пункту 26 проекту Типового договору: “26. Надавач зобов’язаний: ... 5) негайно, але в будь-якому випадку не пізніше ніж протягом трьох годин, повідомляти Користувача про інцидент кібербезпеки, що має (або може мати) значний негативний вплив на надання Послуг, з наданням підтвердження інформування CERT-UA у встановленому законодавством порядку, з подальшим послідовним вичерпним інформуванням Користувача щодо заходів реагування на інцидент кібербезпеки, зокрема щодо	Така вимога про повідомлення протягом трьох годин суперечить пункту 4 Порядку повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних (Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 листопада 2024 № 686) де на такі самі дії відводиться 24 години із поданням додаткової інформації протягом 72 годин: «Про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД, надавач послуг невідкладно, але не пізніше 24 годин з моменту виявлення такого інциденту інформує регулятора комунікаційних послуг та урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA шляхом направлення повідомлення за формою, встановленою додатком до цього Порядку. У разі виявлення додаткової інформації про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД, не відображеної в повідомленні, зазначеному в абзаці другому цього пункту, надавач послуг надсилає таку інформацію регулятору комунікаційних послуг та урядовій команді реагування на комп'ютерні надзвичайні події України CERT-UA не пізніше 72 годин з моменту виявлення інциденту, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД. Додаткова інформація про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг ЦОД, складається у довільній формі та є доповненням до повідомлення, зазначеного в абзаці другому цього пункту.» Пропонується така редакція: “5) негайно, але в будь-якому випадку не пізніше ніж протягом двадцяти чотирьох годин, повідомляти Користувача про інцидент кібербезпеки, що має (або може мати) значний негативний вплив на надання Послуг, з наданням підтвердження інформування CERT-UA у	Відхилено. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 листопада 2024 № 686 буде приведений у відповідність після прийняття постанови.

	виявлених загроз, виявлених наслідків, усунення загроз, звіту щодо аналізу ефективності вжитих заходів з реагування”.	встановленому законодавством порядку, з подальшим послідовним вичерпним інформуванням Користувача щодо заходів реагування на інцидент кібербезпеки, зокрема щодо виявлених загроз, виявлених наслідків, усунення загроз, звіту щодо аналізу ефективності вжитих заходів з реагування.”	
--	---	--	--

***Зауваження та пропозиції від фізичних, юридичних осіб та їх об’єднань надійшли англійською мовою та неофіційно перекладені українською мовою.**