Захист даних в арбітражі

№14, 08 квітня 2021

Євген Блінов ,
партнер, керівник практики міжнародного арбітражу
Eterna Law

Віктор Пасічник ,
молодший юрист
Eterna Law

Упродовж останніх кількох років питання захисту даних у міжнародному арбітражі набуло особливої актуальності. Це передусім пов'язано з набуттям чинності Загальним регламентом про захист даних від 25 травня 2018 року (GDPR) і дедалі ширшим використанням новітніх технологій в арбітражному процесі. З початком пандемії COVID-19 кількість офлайн-слухань значно скоротилась. Натомість набула поширення практика проведення слухань онлайн, навіть у досить великих і складних спорах. Це призвело до збільшення ризику як витоку даних (наприклад, унаслідок кібератаки), так і накладення санкцій із боку відповідних регуляторів за порушення законодавства про захист даних.

Вплив GDPR на міжнародний арбітраж

Набуття чинності GDPR було довгоочікуваною подією, оскільки регламент, по-перше, детально врегулював питання обробки персональних даних, і по-друге, установив екстратериторіальне застосування своїх положень та вимог. Зокрема, вимоги GDPR можна застосовувати й до компаній, що не мають фізичного представництва в ЄС, проте обробляють персональні дані громадян ЄС або, наприклад, таргетують громадян ЄС через вебсайт чи додаток, орієнтований на ринки ЄС.

GDPR надав широке визначення поняттю персональних даних та їх обробки, визначив досить обмежений перелік підстав для обробки даних і встановив істотну відповідальність за порушення правил їх обробки. Так, ст. 83(5) GDPR передбачає можливість накладення адміністративного штрафу до 20 млн євро або в разі застосування санкцій до компанії – до 4 % від загального глобального річного обороту за попередній фінансовий рік, залежно від того, яка сума є вищою. Такі санкції є досить суворими й співмірними зі штрафами, які зазвичай накладають антимонопольні органи як у ЄС, так і в Україні.

Вимоги GDPR підлягають застосуванню як частина матеріального права місця арбітражу, якщо воно знаходиться в межах ЄС. Варто зазначити, що значна частина арбітражних інституцій, що адмініструють спори за участі українських сторін, розташована в межах ЄС, зокрема Міжнародна торговельна палата (ICC) у Франції, Арбітражний інститут торговельної палати Стокгольму (SCC) у

Швеції, Віденський міжнародний арбітражний центр (VIAC) в Австрії. В арбітражних спорах, що адмініструються такими інституціями, вимоги GDPR щодо безпеки даних підлягають застосуванню до всіх учасників процесу. Так, у Примітці щодо проведення арбітражу за правилами ICC ICC зазначає, що у процесі розгляду справи трибунал має вказати учасникам, що до питань захисту даних підлягає застосуванню GDPR, а також те, що вони, беручи участь у процесі, надають згоду на збір, обробку та передачу своїх персональних даних.

Питання застосовності GDPR до арбітражних процесів, що адмініструються інституціями поза межами ЄС, є дещо складнішим. За загальним правилом передання персональних даних громадян ЄС до третіх країн можливе лише за наявності спеціальних запобіжних заходів відповідно до вимог GDPR, що мають на меті забезпечити належний захист таких персональних даних. Наприклад, передання може відбуватися на підставі "рішення про адекватність", затвердженого Європейською комісією, яке підтверджує, що третя країна забезпечує належний рівень захисту персональних даних.

Якщо цього "рішення про адекватність" немає, як у випадку України, належним запобіжником, що дозволяє передавати дані третім країнам, може бути, зокрема, укладання "стандартних контрактних положень" (схвалених Єврокомісією) між організацією чи особою, що передає персональні дані, та організацією чи особою поза межами ЄС, що отримує такі персональні дані (наприклад, між арбітром – громадянином ЄС й арбітром – громадянином України чи арбітражною інституцією, що розташована на території України).

Зрештою, за неможливості застосовувати будь-який із запобіжних заходів GDPR передбачає певні відступлення від загальних правил, які можна використовувати в арбітражі. Так, ст. 49(1)(e) GDPR передбачає можливість передання даних до третіх країн для забезпечення підготовки й подання претензій і позовів, а також захисту від них.

Виходячи з роз'яснення 111 до GDPR, таке передання є можливим у межах позасудових спорів, до яких належать і арбітражі, але тільки за певних умов. Так, GDPR дозволяє лише неповторюване передання даних у законних цілях контролера за умови, що буде збережено рівень захисту персональних даних фізичних осіб, гарантований GDPR. Також рекомендовано звести кількість передаваних даних лише до тих, які є абсолютно необхідними для провадження. Такі дані рекомендовано за можливості псевдонімізувати, а також укласти угоди про конфіденційність під час їх передавання.

Рекомендації щодо захисту даних та інформаційної безпеки

Іншою причиною зростання уваги до питання захисту даних в арбітражі є широке використання новітніх технологій. Через пандемію COVID-19 для розгляду спорів і проведення слухань онлайн використовували програмне забезпечення для проведення відеоконференцій, електронну пошту та хмарні сховища для обміну документами в електронній формі. Попри те, цей формат має свої безумовні переваги, як-от зручність в організації слухань (учасникам не потрібно збиратися в одному місці) й економія коштів для сторін (витрати на програмне забезпечення значно нижчі, ніж на перельоти, проживання та харчування для сторін, їхніх представників й арбітрів, а також ніж на організацію слухань у певному місці), він має свої недоліки. Питання захисту даних і кібербезпеки є одним із найбільш істотних, оскільки конфіденційність є однією з головних переваг міжнародного арбітражу. Її порушення може призвести до істотних негативних наслідків, включно з фінансовими втратами й репутаційною шкодою, а також підірвати репутацію міжнародного арбітражу як безпечного й ефективного способу вирішення спорів.

Наслідками порушення конфіденційності та витоку даних для сторін можуть бути:

1) падіння ціни акцій публічної компанії;

2) падіння інвестиційної привабливості приватної компанії;

3) зменшення можливостей для залучення боргового фінансування та погіршення його умов;

4) утрата наявних і потенційних клієнтів;

5) звільнення топменеджменту;

6) погіршення репутації держави на міжнародній арені та її привабливості для інвесторів (у разі інвестиційного спору);

7) ініціювання розслідувань, зокрема кримінальних, накладення штрафів та інших санкцій;

8) ініціювання спорів контрагентами.

Порушення конфіденційності та витік даних в арбітражному спорі можуть відбутися як унаслідок недбалості осіб, що мають доступ до персональних даних / іншої конфіденційної інформації, так і внаслідок зловмисної діяльності осіб, що бажають отримати доступ до такої інформації. Таку діяльність зазвичай здійснюють за допомогою кібератак. Її мішенями може будь хто з учасників арбітражного процесу, зокрема сторони, їхні юридичні радники, арбітражні інституції, арбітри, інші учасники процесу (свідки, експерти, перекладачі тощо), а також компанії, що забезпечують проведення відеоконференцій, хмарне зберігання електронних документів, обмін електронними повідомленнями.

Арбітражні інституції приділяють значну увагу питанням захисту даних. Так, Лондонський суд міжнародного арбітражу (LCIA) уніс до своїх правил 2020 року нову, окрему статтю, присвячену захисту даних. Так, ст. 30A оновлених правил LCIA передбачає, що за погодженням зі сторонами арбітражний трибунал може розглянути питання щодо доцільності:

– ужиття заходів інформаційної безпеки для захисту фізичної та електронної інформації, поширеної в арбітражі;

– ужиття заходів щодо забезпечення відповідності процесу обробки даних, утворених чи отриманих протягом арбітражу, вимогам законодавства про захист даних.

Водночас LCIA та відповідний арбітражний трибунал уповноважені надавати зобов'язальні для сторін й арбітрів вказівки щодо інформаційної безпеки та захисту даних з урахуванням положень застосовного права.

Міжнародні неурядові організації у сфері міжнародного арбітражу також приділяють значну увагу захисту даних. Вони розробляють і публікують різноманітні гайдлайни, рекомендації та протоколи. Такі норми "м'якого права" відіграють значну роль у міжнародному арбітражі через відносно невелику кількість зобов'язальних правових норм та їхній загальний характер, а також дають змогу зробити процес передбачуванішим.

Прикладом такої норми "м'якого права", що регулює питання захисту даних в арбітражі, є Дорожня карта щодо захисту даних у міжнародному арбітражі, розроблена Міжнародною радою з комерційного арбітражу (ICCA) спільно з Міжнародною асоціацією юристів (IBA) й опублікована в лютому 2020 року. У цій Дорожній карті закріплено принципи обробки персональних даних у міжнародному арбітражі, одним із яких є принцип захисту персональних даних, що передбачає вжиття необхідних технічних та організаційних заходів для захисту персональних даних від ризиків, пов'язаних з їх обробленням (витік, утрата / знищення).

Перелік зазначених технічних та організаційних заходів наведено, зокрема, у Гайдлайні IBA щодо питань кібербезпеки, опублікованому в жовтні 2018 року. У ньому IBA рекомендує вжити низку заходів, зокрема:

1. **У сфері технологій** – регулярно оновлювати програмне забезпечення, використовувати захищене підключення до Інтернету та безпечну електронну пошту, видаляти чи архівувати дані, що більше не є потрібними, робити регулярні бекапи важливих даних (бажано також робити окремі бекапи на фізичному носії). Рекомендовано використовувати шифрування даних і програмне забезпечення, що дає змогу видаляти дані віддалено, на випадок утрати або викрадення їх носія. Також IBA рекомендує створювати для співробітників акаунти з різним рівнем доступу, надаючи їм доступ лише до даних, що необхідні в роботі.

2. **У сфері організаційного процесу** – використовувати складні паролі, що не повторюються, а також багатофакторну автентифікацію. IBA також рекомендує призначити співробітника, відповідального за безпеку даних (data privacy officer). Юридичним фірмам та інституціям рекомендовано розробити політики у сфері захисту даних і кібербезпеки, протокол реагування на витік даних / кібератаку, а також проводити періодичні оцінки ризиків і тестування на проникнення

(penetration testing), проводити регулярне навчання персоналу з питань захисту даних та кібербезпеки.

Іншим важливим документом є опублікований у 2020 році Протокол про кібербезпеку в міжнародному арбітражі, розроблений спільно ICCA, Асоціацією адвокатів м. Нью-Йорк (NYC Bar) і Міжнародним інститутом запобігання і вирішення конфліктів (CPR). Цей Протокол пропонує кілька принципів, зокрема:

1) відповідальність кожного учасника арбітражного процесу за вжиття заходів інформаційної безпеки;

2) ухвалення арбітражним трибуналом рішення щодо вжиття заходів інформаційної безпеки з урахуванням потенційних ризиків, наявних технологій та організаційних практик, обтяжливості та вартості таких заходів і їх співмірності ресурсам сторін й інституції, яка адмініструє, а також ефективності арбітражного процесу;

3) рекомендовано вирішувати питання інформаційної безпеки якомога раніше, зазвичай не пізніше від наради щодо порядку розгляду справи (case management conference);

4) повноваження арбітражного трибуналу на вжиття заходів за своєю ініціативою;

5) повноваження арбітражного трибуналу накладати санкції на сторони у разі порушення правил інформаційної безпеки.

Отже, питання захисту даних у міжнародному арбітражі має істотне значення з огляду на значні ризики в разі витоку даних як із погляду прямих втрат, так і з погляду потенційних регуляторних санкцій. Попри те, що багато питань щодо захисту даних в арбітражі досі залишаються контраверсійними, за останні кілька років було опубліковано серію відповідних рекомендацій. Їх раціональне застосування має зробити процес безпечнішим і передбачуванішим для всіх учасників. А в разі виникнення питань щодо захисту даних в арбітражі ми рекомендуємо задля уникнення можливих негативних наслідків звертатися до висококваліфікованих юристів.