



ПИТАННЯ ЗАХИСТУ ДАНИХ

У разі перенесення, навіть тимчасового, бізнесу з України до Польщі, зазвичай переносяться всі бази даних, включаючи бази даних, в яких обробляються персональні дані. Як гарантувати, що ці бази даних можна буде використовувати на законних підставах? Чи йдісно так істотно впливає зміна країни, де фактично відбувається обробка даних, на можливість використання баз даних, які раніше використовувалися цілком законно? А якщо опрацьовані дані стосуються не громадян ЄС, а лише громадян України? У цій статті ми відповімо на деякі з ключових питань, надавши практичний підхід до обробки даних у новій правовій реальності.

ЗАКОНОДАВЧА БАЗА УКРАЇНИ

Україна, не будучи членом Європейського Союзу чи Європейської економічної зони, має власні нормативні акти, які забезпечують правову основу для обробки персональних даних. Основним нормативним актом є Закон «Про захист персональних даних» від 01.06.2010 № 2297-VI.

Більш того, в Україні немає окремого спеціалізованого органу із захисту даних, як того вимагає Загальний регламент про захист даних («GDPR»). З 1 січня 2014 року Уповноважений Верховної Ради України з прав людини (омбудсмен) був призначений державним органом, відповідальним за контроль за дотриманням законодавства про захист даних, і з того часу Уповноважений прийняв кілька загальнозастосовних наказів, які ефективно виконують покладену на нього роль.

ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ ЗА МЕЖІ УКРАЇНИ

Відповідно до законодавства України персональні дані не можуть оброблятися з метою, відмінною від тієї, з якою вони були зібрані. Таким чином, щодо цього українське законодавство діє так само, як і на території ЄС.

Більше того, законодавство України вимагає, щоб персональні дані могли передаватися лише до країн, які забезпечують адекватний рівень захисту даних. Зокрема, законодавство визначає, що адекватний рівень захисту даних забезпечується:

1. членами Європейської економічної зони,
2. країнами, що приєдналися до Конвенції Ради Європи про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108) - список країн, що підписали Конвенцію, доступний на офіційному сайті Ради Європи:

<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>.

Таким чином, передача персональних даних до Польщі не вимагає додаткових умов, крім законних підстав для обробки.

Важливо, що українське законодавство про захист даних не має "екстериторіальної дії" (тобто не застосовується до суб'єктів за межами України). Українське законодавство не містить жодних посилань на національність/місце проживання осіб, чиї персональні дані підлягають захисту - тому передбачається, що застосовується територіальний принцип, що означає, що захисту підлягають персональні дані, що стосуються всіх осіб, що знаходяться лише на території України.

ОБРОБКА ДАНИХ, ПЕРЕДАНИХ З УКРАЇНИ У ВІДПОВІДНОСТІ З GDPR

Якщо планується транскордонна передача персональних даних, необхідно дотримуватися вимоги стосовно правової підстави для такої передачі. Однак це стосується не тільки правового підґрунтя за українським законодавством; оскільки передача даних здійснюється в країну ЄС, необхідно також знайти відповідну правову підставу для обробки відповідно до GDPR. І це незважаючи на те, що у багатьох випадках дані резидентів ЄС не обробляються.

Це пов'язано з тим, що GDPR застосовується для обробки персональних даних у контексті діяльності установи контролера або процесора в Європейському Союзі. У будь-якому випадку, якщо дані передаються у зв'язку із заснуванням компанії або дочірнього підприємства у Польщі, такі дані мають оброблятися відповідно до GDPR.

Це означає, що якщо база персональних даних була створена в Україні і тепер передається з України з наміром бути використаною установою в Польщі, правова основа для обробки таких даних, яка була дійсна в Україні, тепер має бути перевірена відповідно до стандартів GDPR.

Це стосується особливо чутливих даних, таких, як дані про здоров'я. Відповідно до GDPR вони можуть оброблятися в обмежених випадках, особливо у сфері

зайнятості та соціального забезпечення та законодавства про соціальний захист, якщо це дозволено європейським законодавством або держави-члена. Якщо трудовий договір регулюється законодавством України, то ця правова основа недійсна і, швидше за все, необхідна згода суб'єкта персональних даних (або інша правова підстава).

Ще одним важливим питанням є надання достатнього обсягу інформації відповідно до ст. ст. 13 та 14 GDPR, тому що інформація, що надається суб'єктам даних відповідно до GDPR, значно відрізняється і ширша, ніж інформація, яка має бути подана відповідно до українського законодавства. Зокрема, згідно з українським законодавством, суб'єкт даних має бути поінформований про свої права, які не охоплюють права суб'єктів даних згідно з GDPR, такі як, наприклад, право бути забутим.

ЗВОРОТНА ПЕРЕДАЧА ДАНИХ В УКРАЇНУ

Зворотна передача персональних даних в Україну, швидше за все, може потрапити під суворий режим GDPR щодо передачі даних до третіх країн, оскільки, згідно з GDPR та поточними рішеннями Комісії ЄС, Україна не вважається такою, що забезпечує адекватний рівень захисту.

При оцінці передачі даних у юрисдикції з недостатнім рівнем захисту відповідно до GDPR, такі як Україна, для забезпечення їх безпеки та надійності можна дотримуватися рекомендацій Європейської ради захисту даних, що містять покрокове керівництво:

- Крок 1. Знайте про передачу даних.
- Крок 2. Перевірте метод передачі даних.
- Крок 3. Оцініть законодавство та практику третьої країни (України) – одержувача.

Виконуючи ці кроки, ми, швидше за все, прийдемо до висновку, що стандартні договірні положення (SCC) є найпростішим рішенням для легалізації зворотної передачі даних.

РЕЗЮМЕ

У кожному випадку передачі персональних даних з України в країну-член ЄС, наприклад, Польщу, необхідно вжити заходів для оцінки повної відповідності та, за необхідності, дотримання вимог не лише українського законодавства, а й GDPR. Ми рекомендуємо провести такий аналіз на якомога більш ранній стадії. Таким чином, ми забезпечимо спокій не тільки у разі втручання Польського управління захисту персональних даних, але й насамперед у разі подальшого розвитку компанії, особливо якщо due diligence компанії буде проводитись у зв'язку з наміром знайти інвестора або продати компанію.

Контакти:

У разі виникнення додаткових питань ми рекомендуємо вам зв'язатися з нашими фахівцями:



Анна Матусяк-Векера

Адвокат
Керівник практики захисту даних/
Практика комплаєнсу

anna.matusiak-wekiera@jdp-law.pl



Криштоф Бак

Адвокат
Юрист

krzysztof.bak@jdp-law.pl

Уся інформація в цьому інформаційному бюлетені є безкоштовною. Публікація не носить рекламного характеру та здійснена виключно з інформаційною метою. Інформацію, вказану в цьому матеріалі, не належить розглядати як юридичну консультацію чи комерційну пропозицію, зокрема відповідно до ст. 66 § 1 Цивільного кодексу РП. JDP DRAPALA & PARTNERS Sp. j. цим виключає свою відповідальність щодо будь-яких вимог, збитків чи шкоди, що виникли чи пов'язані з використанням інформації, змісту чи матеріалів, зазначених в інформаційному бюлетені.

Адміністратором даних, обробка яких здійснюється з метою: (i) інформування про виконання професії та пов'язаної діяльності, (ii) листування (iii) архівації є JDP DRAPALA & PARTNERS Sp. j. з місцезнаходженням у Варшаві. Більше інформації на тему обробки персональних даних Адміністратором знайдете [на цьому сайті](#).