

*Тарасюк Антон Володимирович*  
*Національний університет біоресурсів*  
*і природокористування України,*  
*аспірант*

## **ПРОЗОРІСТЬ В РАМКАХ ЗАГАЛЬНОГО РЕГУЛЮВАННЯ ЗАХИСТУ ДАНИХ (GDPR)**

Враховуючи рівень інформатизації та розвитку технологій, приватність (privacy) стає для багатьох правом, що потребує додаткового захисту. Захист персональних даних фізичних осіб та можливість реального впливу фізичних осіб (суб'єктів персональних даних) на умови обробки їх персональних даних в мережі Інтернет в сучасних умовах стають максимально актуальними, особливо, враховуючи розвиток таких технологій як «Великі дані» та «Інтернет речей».

Інформація про той факт, що 87 мільйонів користувачів соціальної мережі Facebook так чи інакше зазнали впливу внаслідок порушення даних (data breach)[1] викликало небувалий резонанс до теми реального впливу суб'єктів персональних даних на реалізацію своїх прав та прозорості обробки їхніх персональних даних. Нові виклики, які ставить перед сучасним суспільством технологічний бізнес призводять до реакції, що виражається у відповідному регулюванні нових або оновлених правовідносин, що виникають завдяки новим технологіям.

В травні 2018 року вступає в силу, прийнятий квітні 2016 року Регламент (ЄС) 2016/679 «Про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних (Загальне регулювання захисту даних (GDPR))[2].

Враховуючи екстериторіальність GDPR, компаніям з усього світу, послуги яких орієнтовані на європейський ринок потрібно дуже уважно підходити до захисту персональних даних, включаючи дотримання умов

прозорості обробки таких даних, як це передбачено у самому GDPR та у відповідних роз'ясненнях.

Говорячи, про принципи прозорості в рамках обробки персональних даних, варто зазначити, що в Україні, основним законом, що регулює захист персональних даних є закон України «Про захист персональних даних»[3]. В статті 6 вказаного закону вказано, що «обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки»[3]. Таким чином, в рамках українського законодавства «прозорість» визначається як одна з умов обробки персональних даних, але деталізація умов «прозорості» відсутня у вказаному законі.

В рамках GDPR, «робоча група 29» (working party 29) надає роз'яснення та Керівні принципи (guidance) з різних питань, що виникають у контролерів та процесорів (як вони визначені в рамках GDPR) щодо різних аспектів застосування вказаного регламенту. Одне з таких роз'яснень стосується «прозорості» під час обробки персональних даних (далі Керівні принципи) [4].

Як вказано у самих Керівних принципах, «прозорість» є всеосяжним обов'язком для контролерів та процесорів (як вони визначені GDPR) і застосовується у наступних трьох ключових сферах:

- 1) Надання інформації суб'єктам персональних даних для чесної обробки
- 2) Умови комунікації контролерів з суб'єктами персональних даних щодо їх прав в рамках GDPR
- 3) забезпечення реалізації прав суб'єктів персональних даних контролерами [4].

Таким чином, виділяється три ключові стадії, в рамках яких суб'єкту персональних даних має бути абсолютно зрозуміло, що відбувається з його персональними даними, хто має або отримує право на їх обробку та на яких

умовах, а також, що саме може зробити такий суб'єкт персональних даних для реальної реалізації своїх прав.

Якщо говорити про практичні аспекти реалізації принципу «прозорості» в рамках обробки персональних даних в Україні, то можна простежити тенденцію занадто складних форм згод на обробку персональних даних. Ба більше, такі форми часто настільки заплутані, що суб'єкти персональних даних не розуміють на що вони погоджуються, навіть у випадку, коли читають такі згоди. Комунікація з обробниками персональних даних (як це передбачено законом України «про захист персональних даних») також досить часто проводиться обробниками у непрозорому ключі, що призводить до проблематичної реалізації своїх прав суб'єктами персональних даних на практиці.

В Керівних принципах наводяться приклади правильної та слабкої (невдалої) комунікації обробників з суб'єктами персональних даних в контексті «прозорості», зокрема наводяться наступні вирази, як приклад:

- 1) «Ми можемо використовувати Ваші персональні дані для розвитку нових сервісів»
- 2) «Ми можемо використовувати Ваші персональні дані для дослідницьких цілей»
- 3) «Ми можемо використовувати Ваші персональні дані для пропонування персоналізованих сервісів»[3].

Всі вищевказані способи комунікації названі прикладами слабкої/невірної практики (poor practice example). Причиною цьому служить «загальність» висловлювань – не вказано, які саме сервіси будуть розвиватись, та як саме в цьому будуть використовуватись персональні дані, не вказано, яке саме дослідження відбудеться та які саме сервіси планується надавати в майбутньому.

Комунікація з суб'єктом персональних даних може також доповнюватись візуальними об'єктами, для кращого та всебічного сприйняття таким суб'єктом інформації. Така умова передбачена статтею 12 GDPR [2].

Ще однією умов прозорості, як це вказано у Керівних принципах, є використання простої мови, яка буде зрозуміла потенційній цільовій аудиторії[4]. Таким чином, в рамках GDPR термін «прозорість» при обробці персональних даних означає реальну можливість для суб'єктів персональних даних розуміти, що і як відбувається з їх персональними даними.

**Висновки:** «прозорість» в рамках GDPR не є певним декларативним принципом, а являє собою систему норм в рамках вказаного регламенту, яка забезпечує реальне розуміння суб'єктами персональних даних умов обробки їх персональних даних та своїх прав в рамках такої обробки. Вважаю, що в рамках українського законодавства є доцільним запозичення кращих практик Європейського союзу щодо реалізації принципу «прозорості» в рамках обробки персональних даних.

### *Список використаної літератури*

1. Facebook to contact 87 million users affected by data breach. Стаття в theguardian.com. [Електронний ресурс] // Режим доступу: <https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach>
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI [Електронний ресурс] // Офіційний веб-сайт Верховної Ради України. - Режим доступу: <http://zakon2.rada.gov.ua/laws/show/2297-17>

4. Guidelines on Transparency under Regulation 2016/679 (wp260rev.01).  
[Электронный ресурс] // режим доступа:  
[http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=622227](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227)