

DIGITAL OMNIBUS – nadchodzące zmiany w RODO

**Alert
prawny**

Co musisz wiedzieć żeby pozostać GDPR compliant?

Komisja Europejska zaproponowała pakiet zmian do RODO („Digital Omnibus”), który ma uprościć i uporządkować przepisy dotyczące ochrony danych osobowych. Celem jest obniżenie kosztów zapewnienia zgodności oraz zwiększenie przejrzystości, bez obniżania poziomu ochrony praw. Zmiany dotyczą m.in. doprecyzowania definicji danych osobowych, ułatwienia stosowania przepisów o DPIA i zgłaszaniu naruszeń oraz wyjaśnienia zasad przetwarzania danych w kontekście systemów AI.

Najważniejsze zmiany

1. Dane osobowe – kiedy dane są „osobowe”?

Informacja nie będzie uznawana za dane osobowe dla danego podmiotu, jeżeli podmiot ten nie ma środków racjonalnie prawdopodobnych do identyfikacji osoby.

Co to oznacza? Jeśli otrzymujesz dane pseudonimizowane i nie masz realnych możliwości identyfikacji osoby, możesz nie być związany RODO w odniesieniu do tych danych.

2. Cookies – koniec z „banner fatigue”

Nowe wymogi:

- Możliwość odrzucenia wszystkich cookies jednym kliknięciem
- Zakaz ponownego wyświetlania banneru przez minimum 6 miesięcy po odmowie
- Obowiązek respektowania zautomatyzowanych, maszynowo czytelnych sygnałów wyboru użytkownika (np. ustawienia przeglądarki)

Co należy zrobić? Zaktualizuj banery cookies – dodaj opcję jednokrotnego odrzucenia wszystkich i przygotuj się na obsługę automatycznych sygnałów z przeglądarek.

3. Zgłaszanie naruszeń – wyższy próg, dłuższy termin

Nowe wymogi:

- Póg zgłoszenia do organu nadzorczego podniesiony z „ryzyka” do „wysokiego ryzyka”, termin wydłużony z 72 do 96 godzin.
- Zgłoszenia dokonywane przez jednolity punkt zgłoszeń (Single Entry Point).

Co to oznacza? Mniej zgłoszeń, więcej czasu na reakcję, ale konieczność oceny „wysokiego ryzyka” według nowych kryteriów.

4. DPIA – ujednolicone listy i wzory

Zamiast różnych krajowych list – jedna unijna lista operacji wymagających DPIA i lista operacji zwolnionych z tego obowiązku.

Co należy zrobić? Poczekaj na nowe listy i wzory, a następnie zaktualizuj swoje procedury DPIA.

5. Obowiązek informacyjny – nowe zwolnienia

W prostych relacjach biznesowych nie będziesz musiał dostarczać szczegółowej klauzuli informacyjnej, jeśli przetwarzasz tylko podstawowe dane osobowe i cel jest oczywisty dla osoby, której te dane dotyczą.

Powyższe nie będzie miało zastosowania gdy: przekazujesz dane innym podmiotom, wysyłasz je poza UE, podejmujesz zautomatyzowane decyzje lub występuje wysokie ryzyko.

Co to oznacza? W prostych relacjach biznesowych możesz nie być zobowiązany dostarczać pełnej klauzuli informacyjnej – ale tylko jeśli spełnisz określone warunki.

6. Nadużycia prawa dostępu

Możliwość odmowy lub pobrania rozsądnej opłaty przy żądaniach nadużywających prawa dostępu (np. w celu wyłudzenia informacji).

Co to oznacza? Łatwiejsza obrona przed żądaniem dostępu składanymi w złej wierze.

7. Przetwarzanie danych dla AI – prawnie uzasadniony interes

Wyraźne potwierdzenie, że przetwarzanie danych osobowych dla rozwoju i działania systemów AI może opierać się na prawnie uzasadnionym interesie, ale w dalszym ciągu przy spełnieniu wymogów i zabezpieczeń określonych dla tej podstawy prawnej.

8. Dane szczególne w AI – nowa derogacja

Dozwolone „resztkowe” przetwarzanie szczególnych kategorii danych przy rozwoju AI, o ile wdrożono skuteczne środki unikania ich zbierania oraz niezwłocznego usuwania albo skutecznego zabezpieczenia, gdy usunięcie wymagałoby niewspółmiernego wysiłku.

Co należy zrobić? Jeśli rozwijasz lub używasz AI przetwarzającego dane osobowe:

- Przeprowadź testy równowagi prawnie uzasadnionego interesu, wdróż minimalizację i filtrację danych, w tym wykrywanie i usuwanie danych szczególnych, oraz adekwatne zabezpieczenia przed wyciekiem danych.
- Zapewnij bezwarunkowe prawo sprzeciwu i wzmocnioną transparentność.

9. Dane biometryczne do weryfikacji tożsamości

Możliwość wykorzystywania danych biometrycznych (np. odcisk palca, Face ID) do weryfikacji tożsamości użytkownika, jeśli dane pozostają w jego urządzeniu lub są zaszyfrowane kluczem, który ma tylko on.

Co to oznacza? Możesz używać biometrii do weryfikacji, jeśli dane biometryczne nie opuszczają urządzenia użytkownika lub są odpowiednio zaszyfrowane.

Jak możemy pomóc?

Gap assessment

Szybka ocena wpływu zmian na Twoją organizację.



Audyt AI governance

Weryfikacja zgodności projektów AI z nowymi wymogami.



Aktualizacja dokumentacji

Klauzule informacyjne oraz wewnętrzne polityki i procedury.



Szkolenia RODO

Szkolenia dla zespołów prawnych, IT i biznesowych.



Kluczowi doradcy

Eksperci z Praktyki Prawa Spółek, Fuzji i Przejęć



Bartosz Marcinkowski

Partner

E: bartosz.marcinkowski@dzp.pl

T: +48 660 440 329



Mateusz Jankowski

Senior Associate

E: mateusz.jankowski@dzp.pl

T: +48 516 294 922