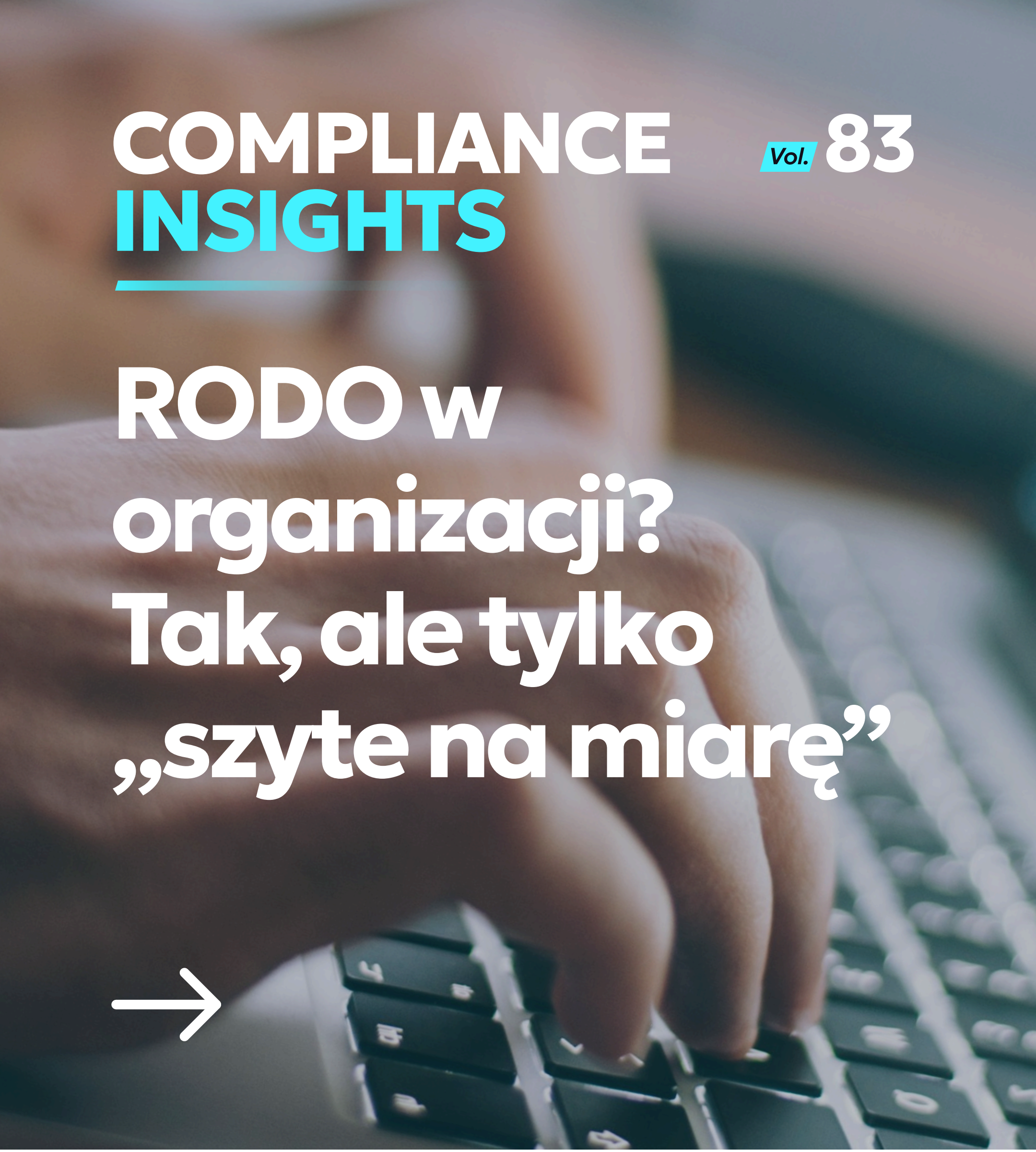
COMPLIANCE INSIGHTS

Vol. 83

RODO w organizacji? Tak, ale tylko „szyte na miarę”



KWKR

Behind Your Growth

1. Kara mała, a wnioski dalekosiężne

W jednej z ostatnich decyzji Prezes Urzędu Ochrony Danych Osobowych nałożył na dom opieki karę pieniężną w wysokości 975 zł. Wysokość kary jest pomijalna, szczególnie w porównaniu do innych, wielomilionowych kar nałożonych na inne podmioty. **Dlaczego zatem warto przyjrzeć się temu rozstrzygnięciu?**

Powód jest prosty - zaprezentowane przez Prezesa UODO stanowisko jest jasnym sygnałem dla całego rynku, iż procedury RODO nie są pisane „do szuflady” i muszą mieć realne powiązanie z praktycznym funkcjonowaniem organizacji administratora danych osobowych.

2. RODO szyte na miarę

W tym przypadku powodem nałożenia kary nie był brak wymaganych procedur i dokumentów, ale brak ich dopasowania do realiów prowadzonej przez administratora danych działalności. Analiza uzasadnienia decyzji pozwala na sformułowanie praktycznych wskazówek w zakresie wdrożenia i funkcjonowania RODO w organizacji:

1) samo posiadanie dokumentacji RODO nie jest wystarczające, jeżeli nie uwzględnia ona specyfiki branży, faktycznego sposobu funkcjonowania, skali organizacji, a także rodzaju i zakresu prowadzonego przetwarzania. Kupienie gotowych wzorów z Internetu może być tańsze, ale nie zabezpiecza właściwie ani przetwarzanych danych ani samego administratora;

2. RODO szyte na miarę

2) wydawane członkom personelu upoważnienia do przetwarzania danych powinny odzwierciedlać faktyczny zakres zadań danego pracownika, a więc precyzować kto, do jakich danych i w jakim celu ma dostęp do danych;

3) szkolenie pracowników jest obowiązkiem każdego podmiotu przetwarzającego dane. Aby zapewnić odpowiedni poziom świadomości szkolenia powinny być prowadzone regularnie i obejmować cały personel;

2. RODO szyte na miarę

4) przy realizacji obowiązku informacyjnego kluczowe jest zachowanie zasad wynikających z motywu 39 RODO, przede wszystkim informacje muszą być przekazywane w sposób jasny, precyzyjny i czytelny. W szczególności, w ocenie Prezesa UODO nie jest wystarczające poprzestanie na samym wskazaniu praw wynikających z RODO bez dodania czytelnych informacji na temat tego, w jakich przypadkach osoba, której dane są przetwarzane, może z takich praw skorzystać.

3. Analiza ryzyka nie jest tylko formalnością

Uzasadnienie przedmiotowej decyzji formułuje także istotne wytyczne w zakresie prowadzenia analizy ryzyka:

1) analiza ryzyka stanowi fundament systemu ochrony danych osobowych - nie może być traktowana jako formalność czy zwykły dodatek do dokumentacji, lecz jako punkt wyjścia dla projektowania całego procesu przetwarzania zgodnie z zasadą „privacy by design”;

3. Analiza ryzyka nie jest tylko formalnością

2) analiza musi opierać się na konkretnych, mierzalnych parametrach – powinna opierać się na konkretnych scenariuszach potencjalnych zagrożeń, a nie na ogólnych hasłach czy utartych sloganach. Jej nieodłącznym elementem jest identyfikacja i uwzględnienie charakteru realnie występujących procesów przetwarzania, posiadanych aktywów, potencjalnych zagrożeń oraz faktycznie istniejących środków bezpieczeństwa w ramach zachodzących procesów;

3. Analiza ryzyka nie jest tylko formalnością

3) analiza nie może być wyłącznie szablonowa i oparta na ogólnikach - powinna wynikać z istniejącego stanu faktycznego i odnosić się do rzeczywistych procesów przetwarzania danych. Koniecznym jej etapem jest nie tylko wskazanie istniejących zabezpieczeń, lecz także ocena ich skuteczności w odniesieniu do zidentyfikowanych zagrożeń. Dla organizacji w praktyce oznacza to nie tylko ustalenie jakie środki mają dane chronić, ale także weryfikację, czy są efektywne i zapewniają oczekiwany poziom ochrony;

3. Analiza ryzyka nie jest tylko formalnością

4) brak zarządzania analizą ryzyka oznacza pozorność ochrony danych – Proces dalszego postępowania z analizą jest równie istotny jak jej pierwotne prowadzenie. Wymaga ona aktualizacji, okresowej analizy i przeglądu, a także testowania zastosowanych zabezpieczeń danych oraz w razie konieczności ich doskonalenia;

5) analiza musi być udokumentowana - w perspektywie wynikającej z art. 5 ust. 2 RODO zasady rozliczności, konieczne jest dokumentowanie prowadzonej analizy.

4. Wnioski praktyczne dla przedsiębiorców

Przedmiotowa decyzja potwierdza, że sam fakt posiadania dokumentacji RODO nie gwarantuje bezpieczeństwa prawnego. Jakość dokumentacji, jej dopasowanie do danej organizacji oraz fakt i sposób realnego wdrożenia są kluczowe dla zapewnienia bezpieczeństwa danych. Jednostkowa, symboliczna wysokość kary w omawianej sprawie nie powinna być traktowana jako przyzwolenie dla nieefektywnego i pozornego wdrażania RODO w naszej organizacji.

Kontakt

Mariusz Purgał
Partner
mariusz.purgal@kwkr.pl

Anna Bartosiak
Associate
anna.bartosiak@kwkr.pl

Zespół Compliance KWKR

Michał Hady

Justyna Staszkiewicz-Maj

Anna Rybicka

Jakub Miśkiewicz

Katarzyna Kanik

Joanna Bochaczyk

Maksymilian Skrzypek

Kamil Szymański

KWKR.

Behind Your *Growth*