Warszawa, 9.04.2025 r.

Czy RODO powinno być dostosowane do wielkości firmy? Krytyczna analiza propozycji deregulacyjnych

Propozycje zespołu "SprawdzaMY - Przedsiębiorcy dla Polski" kierowanego przez Rafała Brzoskę dotyczące ograniczenia obowiązków wynikających z RODO dla mniejszych firm wzbudzają uzasadnione kontrowersje. Choć argumenty o nadmiernych obciążeniach administracyjnych brzmią przekonująco, głębsza analiza prawna ujawnia fundamentalne nieporozumienia dotyczące istoty ochrony danych osobowych oraz potencjalne zagrożenia takiego podejścia.

Błędne rozumienie istoty RODO i jego celów

Najbardziej uderzające w tej propozycji jest zawężenie RODO głównie do kwestii obowiązków informacyjnych i klauzul, które rzekomo są "zbyt długie". To fundamentalne niezrozumienie istoty rozporządzenia. Jak wynika z art. 1 ust. 2 RODO, rozporządzenie chroni "*podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych*".

W motywie 13 preambuły RODO prawodawca wskazał wprost, że: "*Aby zapewnić spójny i wysoki stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych*". Nie przewidziano tu żadnego różnicowania ze względu na wielkość podmiotu przetwarzającego dane.

Obowiązki informacyjne stanowią jedynie wierzchołek góry lodowej - widzialny element całego systemu ochrony, ale nie jego istotę. Kluczowe zasady RODO, określone w art. 5, takie jak:

- zgodność z prawem, rzetelność i przejrzystość
- ograniczenie celu
- minimalizacja danych
- prawidłowość
- ograniczenie przechowywania
- integralność i poufność
- rozliczalność

mają na celu zapewnienie bezpieczeństwa danych bez względu na skalę działania przedsiębiorstwa.

Skala działalności a skala przetwarzanych danych

Mały sklep internetowy prowadzony przez mikroprzedsiębiorcę może przetwarzać dane setek czy nawet setek tysięcy klientów.
Co więcej, to właśnie małe firmy często nie dysponują odpowiednimi zasobami lub wiedzą, by skutecznie zabezpieczać dane. Potwierdzają to wyniki badań Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA). W najnowszym Raporcie z 2024 roku zatytułowanym „Report on the State of Cybersecurity in the Union", ENISA wskazała m.in. na istotne luki w cyberbezpieczeństwie małych i średnich przedsiębiorstw (MŚP) w porównaniu do dużych firm, w tym:

- niższy poziom higieny cybernetycznej
- mniejszą świadomość zagrożeń
- niedostateczne raportowanie incydentów
- brak odpowiednich zasobów (np. Centra Operacji Bezpieczeństwa)
- słabsze polityki zarządzania ryzykiem łańcucha dostaw (53% MŚP vs 85% dużych firm)

Raport zaleca wzmocnienie wsparcia technicznego i finansowego dla podmiotów objętych dyrektywą NIS2 oraz ustanowienie zunifikowanego podejścia do szkoleń i budowania świadomości w zakresie cyberbezpieczeństwa.

Problematyczna rola Inspektorów Ochrony Danych (IOD)

Warto zwrócić szczególną uwagę na to, jak restrykcyjne podejście Urzędu Ochrony Danych Osobowych (UODO) do obowiązków Inspektorów Ochrony Danych dodatkowo utrudnia mniejszym przedsiębiorcom wypełnianie wymogów RODO. Problem ten można zaobserwować chociażby na podstawie niedawno opublikowanego poradnika prezesa UODO "Obowiązki administratorów związane z naruszeniami ochrony danych osobowych".
Mimo że UODO definiuje IOD jako "profesjonalnych doradców wspierających administratorów i podmioty przetwarzające w zapewnieniu zgodności z przepisami RODO", to jednocześnie drastycznie ogranicza ich faktyczne możliwości działania. Zgodnie z wytycznymi UODO, inspektorzy nie mogą:

- zgłaszać naruszeń ochrony danych osobowych prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń
- zawiadamiać w imieniu administratorów osób, których dane dotyczą, o naruszeniach
- dokumentować naruszeń ochrony danych osobowych w imieniu administratorów
- podejmować zobowiązań dotyczących bezpieczeństwa przetwarzania w imieniu administratorów

- działać na podstawie pełnomocnictwa w sprawach dotyczących ochrony danych osobowych

W praktyce oznacza to, że w procesie naruszeń ochrony danych osobowych IOD nie może podejmować prawie żadnych czynności wykonawczych. Inspektorzy są ograniczeni do funkcji doradczych i monitorujących, co w wielu organizacjach powoduje konieczność utworzenia odrębnego pionu wykonawczego zajmującego się ochroną danych.

Takie podejście UODO wynika z niezwykle restrykcyjnej wykładni obowiązku unikania przez IOD konfliktu interesów. Organ stoi na stanowisku, że IOD wykonujący obowiązki spoczywające na administratorach lub podmiotach przetwarzających mogą tracić obiektywizm i popadać w konflikt interesów. Oznacza to, że praktycznie każdy udział IOD w realizacji jakiegokolwiek obowiązku nałożonego w RODO na administratora jest według UODO potencjalnym źródłem konfliktu.

Przyjęcie w praktyce takiego poglądu może prowadzić do wyeliminowania IOD z procesu naruszeń ochrony danych. Ograniczenie ich roli wyłącznie do "monitorowania" skutkuje tym, że wszelkie czynności związane z obsługą naruszenia musi wykonywać inny podmiot niż IOD.

Szczególnie problematyczne jest to dla małych i średnich przedsiębiorstw, gdzie IOD często jest jedyną osobą specjalizującą się w ochronie danych osobowych. Wdrożenie stanowiska prezesa UODO wymaga, aby naruszeniem ochrony danych zajmowały się co najmniej dwa piony: jeden wykonawczy, a drugi to IOD. W praktyce, w niewielkich jednostkach z przyczyn ekonomicznych, w których dotychczas IOD był jedyną osobą specjalizującą się w przedmiocie danych osobowych, staje się to trudne do realizacji lub nawet niemożliwe do wykonania.

W konsekwencji powstaje paradoksalna sytuacja, w której to, co miało być wsparciem dla administratorów danych (stanowisko IOD), staje się dodatkowym obciążeniem organizacyjnym i finansowym. Dla małych firm oznacza to konieczność albo zatrudnienia dodatkowych specjalistów od ochrony danych (co zwiększa koszty), albo funkcjonowania w szarej strefie, gdzie IOD formalnie tylko "rekomenduje" działania, a faktycznie je wykonuje, narażając się na potencjalne sankcje ze strony UODO.

To pokazuje fundamentalny problem obecnego podejścia do ochrony danych osobowych w Polsce - zamiast wspierać przedsiębiorców w skutecznym wdrażaniu mechanizmów ochrony danych, regulacje i ich interpretacje tworzą dodatkowe bariery. Dla małych i średnich przedsiębiorstw, które dysponują ograniczonymi zasobami, stanowi to poważne wyzwanie.

Analiza art. 23 RODO w kontekście propozycji deregulacyjnych

Zespół kierowany przez Rafała Brzoskę argumentuje za ograniczeniem obowiązków informacyjnych dla mniejszych przedsiębiorców. Propozycja ta wymaga analizy w świetle art. 23 RODO, który dotyczy możliwości ograniczenia niektórych obowiązków i praw przewidzianych w rozporządzeniu.

Art. 23 RODO pozwala państwom członkowskim na wprowadzenie w swoim prawie krajowym pewnych ograniczeń w stosowaniu wybranych przepisów rozporządzenia (art. 12-22, art. 34 oraz art. 5). Na pierwszy rzut oka mogłoby się wydawać, że przepis ten otwiera drogę do postulowanych przez zespół Brzoski ograniczeń. Jednak dokładna analiza warunków z art. 23 ust. 1 RODO prowadzi do innych wniosków.

Po pierwsze, art. 23 RODO zawiera zamknięty katalog celów, dla których możliwe jest wprowadzenie ograniczeń. Są to m.in.:

- bezpieczeństwo narodowe
- obronność
- bezpieczeństwo publiczne
- zapobieganie przestępczości
- inne ważne cele leżące w ogólnym interesie publicznym Unii lub państwa członkowskiego
- funkcje kontrolne związane ze sprawowaniem władzy publicznej
- ochrona osoby, której dane dotyczą, lub praw i wolności innych osób
- egzekucja roszczeń cywilnoprawnych

Na liście tej nie ma ułatwienia prowadzenia działalności gospodarczej ani zmniejszenia obciążeń administracyjnych dla określonych kategorii przedsiębiorców.

Po drugie, zgodnie z art. 23 ust. 1 RODO, każde ograniczenie musi szanować istotę podstawowych praw i wolności oraz musi być niezbędnym i proporcjonalnym środkiem w demokratycznym społeczeństwie. Test proporcjonalności wymaga wykazania, że:

- środek jest odpowiedni do osiągnięcia zamierzonego celu
- nie istnieją mniej restrykcyjne środki, które pozwoliłyby osiągnąć ten sam cel
- korzyści wynikające z ograniczenia przeważają nad negatywnymi skutkami dla ochrony danych

Po trzecie, art. 23 ust. 2 RODO wymaga, aby akty prawne wprowadzające takie ograniczenia zawierały szczegółowe przepisy dotyczące m.in. celów przetwarzania, zakresu wprowadzonych ograniczeń, zabezpieczeń zapobiegających nadużyciom oraz kategorii administratorów, których dotyczą. Pokazuje to, że nawet dopuszczalne ograniczenia muszą być precyzyjnie określone i nie mogą prowadzić do ogólnego obniżenia standardów ochrony danych.

Europejska Rada Ochrony Danych w swoich wytycznych dotyczących art. 23 RODO (Wytyczne 10/2020) podkreśla, że przepis ten należy interpretować wąsko, a wprowadzane na jego podstawie ograniczenia nie mogą podważać ogólnej skuteczności przepisów o ochronie danych osobowych.
Z powyższej analizy wynika, że art. 23 RODO nie może służyć jako podstawa prawna do generalnego wyłączenia mikro- i małych przedsiębiorców z obowiązków wynikających z RODO wyłącznie ze względu na wielkość przedsiębiorstwa. Ograniczenia takie prawdopodobnie nie realizowałyby żadnego z celów wymienionych w zamkniętym katalogu z art. 23 ust. 1 RODO i nie spełniłyby testu proporcjonalności. Ochrona danych osobowych jako prawo podstawowe nie może być różnicowana ze względu na wielkość podmiotu przetwarzającego dane.

RODO już uwzględnia skalę przetwarzania, nie wielkość podmiotu

RODO już obecnie zawiera mechanizmy dostosowujące wymogi do charakteru i skali przetwarzania danych. W art. 30 ust. 5 RODO wyraźnie zwalnia organizacje zatrudniające mniej niż 250 osób z obowiązku prowadzenia rejestru czynności przetwarzania, o ile przetwarzanie nie stanowi ryzyka dla praw i wolności osób, których dane dotyczą, nie jest sporadyczne lub nie obejmuje szczególnych kategorii danych.
Motyw 13 preambuły RODO stanowi, że: "*Aby uwzględnić szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, niniejsze rozporządzenie przewiduje wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników*".
Co jednak istotne, RODO opiera się na podejściu opartym na ryzyku, które uzależnia poziom ochrony od charakteru, zakresu, kontekstu i celów przetwarzania oraz od skali samego przetwarzania danych, a nie od wielkości podmiotu. Widać to wyraźnie w art. 35 dotyczącym oceny skutków dla ochrony danych (DPIA), gdzie decydującym czynnikiem jest to, czy przetwarzanie "z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych".
Rozporządzenie w art. 35 ust. 3 wskazuje sytuacje, w których ocena skutków jest obowiązkowa, w tym "systematyczną, kompleksową ocenę czynników osobowych odnoszących się do osób fizycznych" czy "przetwarzanie na dużą skalę szczególnych kategorii danych". Nigdzie w tym kontekście nie pojawia się odniesienie do wielkości administratora danych jako czynnika decydującego o konieczności przeprowadzenia DPIA.
Oznacza to, że mikroprzedsiębiorca prowadzący sklep internetowy obsługujący setki tysięcy klientów będzie musiał spełnić te same wymogi co duża korporacja przetwarzająca podobny wolumen danych w podobnym celu. To logiczne podejście, gdyż z perspektywy osoby, której dane są przetwarzane, wielkość przedsiębiorstwa

nie ma znaczenia dla potencjalnych zagrożeń związanych z przetwarzaniem jej danych.
Podejście oparte na ryzyku naturalnie prowadzi do proporcjonalnego dostosowania obowiązków do skali i charakteru przetwarzania. Wyłączenie mikro- i małych przedsiębiorców z określonych obowiązków tylko ze względu na ich wielkość, bez uwzględnienia skali przetwarzania danych, przeczyłoby tej fundamentalnej zasadzie RODO.

Błędne rozumienie obowiązków informacyjnych

Propozycje zespołu Brzoski koncentrują się na ograniczeniu obowiązków informacyjnych, uznając je za zbyt rozbudowane. Tymczasem art. 12 ust. 1 RODO wymaga, aby informacje były przekazywane "*w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem*".
EROD w swoich wytycznych dotyczących przejrzystości (WP260 rev.01) wyraźnie zaznacza, że "*wymóg, aby informacje były 'zwięzłe i przejrzyste', oznacza, że administratorzy danych powinni je przedstawiać w sposób efektywny i zwięzły, aby uniknąć zmęczenia informacyjnego*".
Jeśli klauzule informacyjne są zbyt długie i skomplikowane, to stanowi to naruszenie RODO, a nie jego prawidłowe stosowanie. Problem leży więc nie w samym rozporządzeniu, ale w jego niewłaściwej implementacji przez administratorów danych.

Perspektywa unijna

Dyskusja o potencjalnych zmianach w RODO toczy się również na poziomie Unii Europejskiej. Komisja Europejska w swoim raporcie z 24 czerwca 2020 r. dotyczącym ewaluacji RODO (COM(2020) 264 final) uznała, że:
„*...zgodnie z podejściem opartym na analizie ryzyka przyznawanie odstępstw na podstawie wielkości operatorów nie byłoby podejściem właściwym, ponieważ ich rozmiar sam w sobie nie stanowi wskaźnika ryzyka, jakie przetwarzanie danych osobowych, którego to przedsiębiorstwo się podejmuje, może stworzyć dla osób fizycznych. Kilka organów ochrony danych dostarczyło praktyczne narzędzia ułatwiających wdrożenie RODO przez MŚP prowadzące działalność w zakresie przetwarzania o niskim ryzyku. Wysiłki te powinny zostać zintensyfikowane i rozpowszechnione, najlepiej w ramach wspólnego europejskiego podejścia, aby nie tworzyć barier dla jednolitego rynku*".
Komisja wyraźnie wskazuje więc, że rozwiązaniem problemu nie jest deregulacja, ale lepsze wsparcie dla MŚP w zakresie wdrażania istniejących przepisów.

Realne wyzwania i rozwiązania zgodne z prawem UE

Nie można zaprzeczyć, że wdrożenie RODO stanowi wyzwanie dla mniejszych firm. Jednak zamiast osłabiać ochronę danych osobowych, należałoby skupić się na:

1. Rozwijaniu prostych, praktycznych narzędzi i szablonów dostosowanych do potrzeb małych firm - zgodnie z art. 57 ust. 1 lit. b) RODO, który zobowiązuje organy nadzorcze do promowania świadomości administratorów i podmiotów przetwarzających dotyczącej ich obowiązków.
2. Zwiększaniu dostępności szkoleń i materiałów edukacyjnych - art. 57 ust. 1 lit. d) RODO nakłada na organy nadzorcze obowiązek upowszechniania wiedzy o RODO.
3. Zapewnieniu wsparcia technicznego i prawnego dla mikro- i małych przedsiębiorców - zgodnie z motywem 132 preambuły RODO, organy nadzorcze powinny uwzględniać szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.
4. Promowaniu kodeksów postępowania zgodnie z art. 40 RODO, które mogą być opracowane specjalnie dla mikro-, małych i średnich przedsiębiorców.
5. Zmianie podejścia do roli Inspektorów Ochrony Danych (IOD), tak aby faktycznie wspierali administratorów w realizacji obowiązków wynikających z RODO, ze szczególnym uwzględnieniem specyfiki małych i średnich przedsiębiorstw.

Podsumowanie

Propozycja "RODO dla małych firm" opiera się na błędnym założeniu, że wielkość firmy determinuje potrzebę ochrony danych osobowych. W świetle prawa UE to charakter i skala przetwarzania danych, a nie wielkość przedsiębiorstwa, powinny określać poziom zabezpieczeń.

Zamiast deregulacji, która mogłaby zagrozić prawom obywateli i być potencjalnie niezgodna z prawem pierwotnym UE, potrzebujemy lepszych **narzędzi wsparcia i edukacji dla mniejszych podmiotów.** RODO to nie tylko klauzule informacyjne czy dokumentacja - to kompleksowy system ochrony podstawowych praw obywatelskich w erze cyfrowej, oparty na art. 8 Karty Praw Podstawowych UE oraz art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej.

Magdalena Jacolik – specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.

Źródła:

1. European Union Agency for Cybersecurity (ENISA), "2024 Report on the State of Cybersecurity in the Union", s. 8, dostępny na stronie: https://www.enisa.europa.eu.

2. Europejska Rada Ochrony Danych, "Wytyczne 10/2020 w sprawie ograniczeń na podstawie art. 23 RODO", przyjęte 13 października 2021 r., s. 6-7.
3. Komunikat Komisji do Parlamentu Europejskiego i Rady, "Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejście UE do transformacji cyfrowej -- dwa lata stosowania ogólnego rozporządzenia o ochronie danych", COM(2020) 264 final z 24.6.2020 r., s. 11.