Your World First

C/M/S/

Law . Tax

Zmiany w unijnym prawie ochrony danych osobowych – nowe wyzwania i szanse dla przedsiębiorstw

Raport kancelarii CMS

Maj 2016 r.

Rozporządzenie ogólne o ochronie danych osobowych

Istotne informacje

4 maja 2016 r. – publikacja nowego prawa

25 maja 2016 r. – wejście w życie

Czas na dostosowanie: **2 lata**

Dotyczy: **wszystkich przedsiębiorstw działających na terenie Unii Europejskiej**

Nowy proces w firmie: **Ocena wpływu na prywatność**

25 maja 2018 r. – od tej daty nowe prawo będzie egzekwowane

Kary za niedostosowanie się: **do 20 mln euro lub 4% globalnego rocznego obrotu** z poprzedniego roku finansowego

Spis treści

Większa ochrona, nowe możliwości

Wszyscy działający w Polsce przedsiębiorcy będą musieli dostosować swoją działalność gospodarczą do nowego unijnego prawa – Rozporządzenia ogólnego o ochronie danych osobowych, które będzie miało zastosowanie od 25 maja 2018 r.

Najważniejsze wnioski z lektury rozporządzenia można sprowadzić do dwóch zasadniczych tez. Po pierwsze, ochrona prywatności jest uznawana przez unijnego ustawodawcę za fundamentalne prawo każdego, kogo dane dotyczą, a rolą organów nadzoru jest maksymalizacja tej ochrony za pomocą szerokich prerogatyw wynikających z nowych przepisów.

Po drugie, rozporządzenie otwiera przed przedsiębiorcami nowe możliwości przetwarzania danych do celów biznesowych – precyzyjnie wskazując na przykład, w jaki sposób zgodnie z prawem profilować klientów, choćby na potrzeby zwiększenia sprzedaży. Odpowiada także na trudne pytania, w tym jak przetwarzać dane osobowe dzieci albo w jaki sposób oceniać wpływ przetwarzania danych na prowadzoną działalność.

Czy biznes jest gotowy na tak głęboką zmianę przepisów? Zapytaliśmy o to w naszym badaniu. Wynikom zaprezentowanym w niniejszym raporcie towarzyszą nieodzowne dla każdego przedsiębiorcy informacje dotyczące zakresu zmian w prawie, ich konsekwencji dla biznesu i działań niezbędnych do uzyskania zgodności z nowym rozporządzeniem.

Zapraszamy do lektury!

r.pr. Tomasz Koryzma
Partner
T +48 22 520 8479
E tomasz.koryzma@cms-cmck.com

r.pr. Marcin Lewoszewski
Senior Associate
T +48 22 520 5525
E marcin.lewoszewski@cms-cmck.com

Biznes a nowe regulacje

Nowe unijne przepisy o ochronie danych osobowych oznaczają dla firm nowe obowiązki oraz intensywny proces przygotowania się do ich wypełniania. Czy przedsiębiorcy przetwarzający dane osobowe są na to przygotowani? Jaki jest ich poziom wiedzy o zmianie prawa?

Na kolejnych stronach przedstawiamy raport na temat stanu świadomości polskiego biznesu w zakresie zmieniających się przepisów ochrony danych osobowych, konsekwencji wynikających z tej zmiany oraz planowanych działań.

Raport opiera się na danych uzyskanych z autorskiego badania przeprowadzonego w okresie od kwietnia do maja 2016 r. wśród przedstawicieli ponad 100 przedsiębiorstw działających na terenie Polski w branżach, na które zmieniające się przepisy będą mieć największy wpływ.

Niemal połowa ankietowanych (48%) pracuje w firmach zatrudniających powyżej 500 osób, a 68% to pracownicy firm międzynarodowych.

Najliczniej reprezentowane były branże: ubezpieczeniowa (19%), bankowa (14%) oraz technologiczna (11%). Pokaźną grupę stanowili również przedstawiciele branży FMCG, telekomunikacyjnej, motoryzacyjnej i e-commerce.

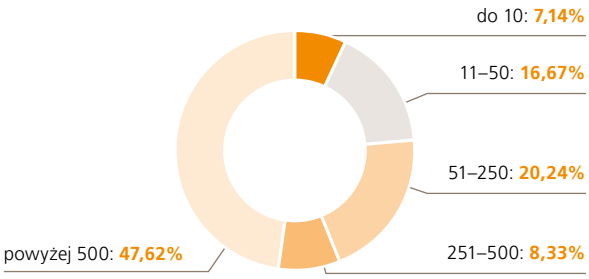
Respondenci to głównie członkowie zarządu oraz dyrektorzy i kierownicy działów. Większość z nich pracuje w dziale prawnym (29%) i IT (11%), zaraz za nimi znaleźli się przedstawiciele działów compliance, bezpieczeństwa, sprzedaży i marketingu.

Wnioski z badania podzieliliśmy na cztery rozdziały:

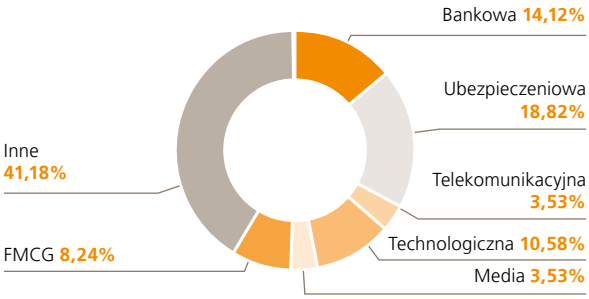
I. Świadomość zmiany
II. Świadomość konsekwencji
III. Planowane działania
IV. Postrzeganie sytuacji

Uczestnicy badania CMS:

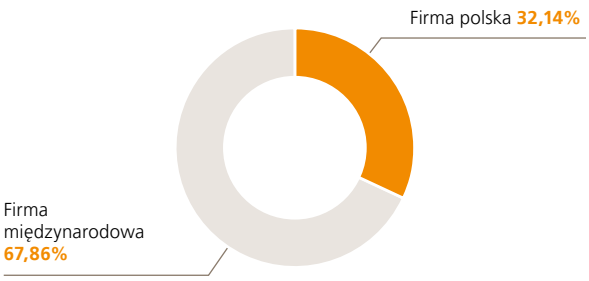
Liczba zatrudnionych osób w firmie



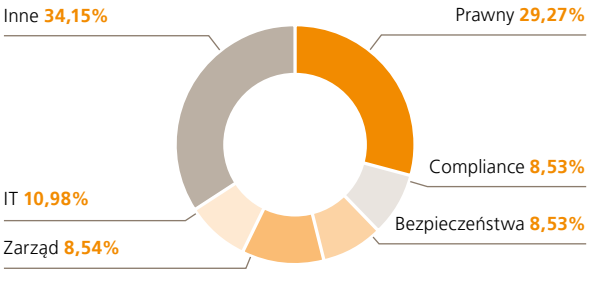
Sektor/branża, w której działa firma



Zasięg działania firmy



Dział, w którym zatrudniony jest respondent




WEB DESIGN
FINANCE

I. Świadomość zmiany

Wynik badania potwierdza, że przedsiębiorcy w zdecydowanej większości są świadomi nadchodzących zmian w unijnym prawie ochrony danych osobowych. Biorąc pod uwagę skalę tych zmian, to zjawisko pozytywne.

Jednocześnie, co mogą sugerować wyniki badania, wiedza przedsiębiorców na temat istoty nowej regulacji i jej konsekwencji dla prowadzonego biznesu jest raczej powierzchowna.

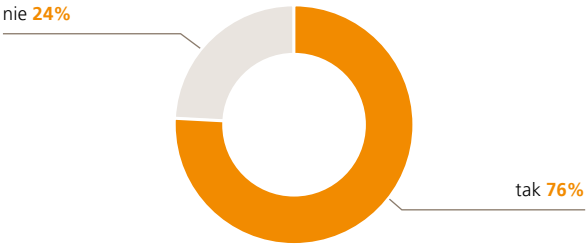
Czas już płynie

Znakomita większość przedsiębiorców ma wiedzę co do stosunkowo krótkiego, bo dwuletniego okresu, który dał im ustawodawca unijny na dostosowanie prowadzonej działalności do nowych przepisów.

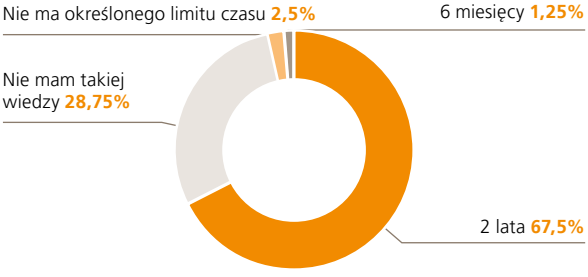
» Ujednolicenie regulacji uprości prowadzenie biznesu w Unii Europejskiej.

uczestnik badania CMS

Czy ma Pani/Pan świadomość, że w maju 2016 r. wejdą w życie nowe europejskie regulacje dotyczące ochrony danych osobowych, nakładające na przedsiębiorców szereg nowych obowiązków?



Czy wie Pani/Pan, jaki czas będą mieli przedsiębiorcy na dostosowanie się do nowego prawa?



II. Świadomość konsekwencji

Przedsiębiorcy poprawnie identyfikują sfery działalności gospodarczej, które są najbardziej podatne na nadchodzące zmiany. Obszary te można sprowadzić do wspólnego mianownika: dane osobowe klientów.

To właśnie działy sprzedaży, marketingu, obsługi klienta, bezpośrednio przetwarzające dane klientów, były najczęściej wymieniane jako te, które wymagają największych zmian w związku z nowymi regulacjami. Znaczna grupa badanych zaznaczyła również działy HR przetwarzające dane pracowników.

Rozporządzenie ogólne o ochronie danych osobowych drastycznie zwiększy sankcje za nieprzestrzeganie przepisów ochrony danych osobowych. Respondenci słusznie wskazali, że potencjalne sankcje mogą sięgać kwot niebagatelnych dla każdego przedsiębiorcy, tj. nawet 4% globalnego rocznego obrotu z poprzedniego roku finansowego albo 20 mln euro – w zależności od tego, która z tych kwot jest wyższa.

Koszty w górę?

Nowe rozporządzenie unijne znacznie rozszerzy obowiązki podmiotów przetwarzających dane osobowe. Zdaniem ankietowanych może wiązać się to ze zwiększeniem kosztów prowadzonej działalności, choćby ze względu na konieczność wdrożenia profesjonalnych systemów ochrony przetwarzanych danych czy bardziej starannego dobierania podmiotów, które przetwarzają dane na zlecenie (np. w centrach usług księgowych czy IT).

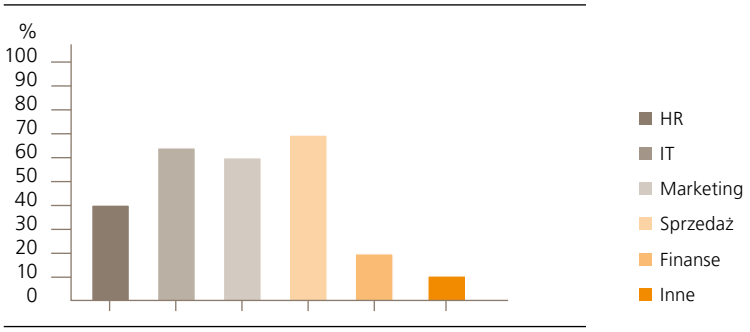
Zwolennicy zmiany pozytywnie oceniają ujednolicenie i spójność przepisów oraz urealnienie ochrony danych osobowych. Sceptycy wyrażają swoje zaniepokojenie potencjalnym wpływem rozporządzenia unijnego na zmniejszenie zaufania klientów. Ich zdaniem przepisy są za ogólne, nakładają na firmy zbyt wiele obowiązków, a konieczność przekazywania klientom rozbudowanych, zawiłych klauzul może spowodować spadek ich zaufania.

Na tym etapie ocena wpływu rozporządzenia na zaufanie klientów może być przedwczesna, gdyż kluczowe znaczenie będzie miała praktyka wykonywania obowiązków przez przedsiębiorców.

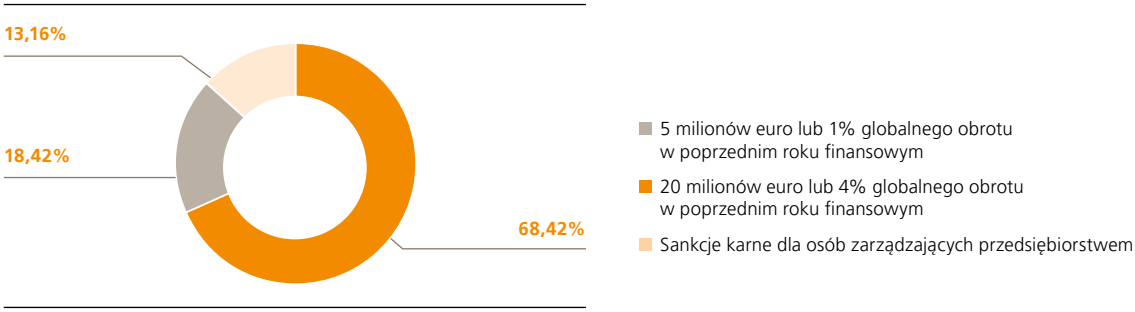
Nowe szanse

Zwraca uwagę fakt, że w nowym prawie szansę dla rozwoju swojego biznesu dostrzega zaledwie niewielka grupa ankietowanych. Może to oznaczać, że wykorzystywanie narzędzi, takich jak Big Data czy profilowanie klientów, nie zagościło jeszcze w Polsce na dobre.

Bazując na Pani/Pana doświadczeniu, które z obszarów biznesowych wymagają największych zmian w związku z nowymi regulacjami?



Czy wie Pani/Pan, jakie sankcje grożą przedsiębiorcom za niedostosowanie działalności do nowych przepisów o ochronie danych osobowych?



Czy w Pani/Pana ocenie wdrożenie nowych europejskich regulacji dotyczących ochrony danych osobowych spowoduje:

III. Planowane działania

Ankietowani przedsiębiorcy intensywnie zapoznają się z nowymi regulacjami, ale większość z nich na tym poprzestaje.

Niewielu przedsiębiorców podjęło inne czynności przygotowawcze, choćby takie, jak zmapowanie procesów biznesowych, które należy ocenić pod kątem nowych przepisów i wyciągnąć wnioski co do koniecznych zmian. Również niewielu przedsiębiorców zdecydowało się na weryfikacje listy dostawców usług, którzy mają dostęp do danych osobowych.

Taki wynik może zaskakiwać z kilku powodów – przede wszystkim dlatego, że nowe rozporządzenie wymusi konieczność renegocjowania umów z tego rodzaju podmiotami albo nawet spowoduje zakończenie z nimi współpracy. To oczywiście może wymagać poniesienia dodatkowych kosztów przez przedsiębiorców.

Ludzie i systemy

Podobnie dostosowanie systemów IT będzie wymagało wielu analiz, negocjacji z dostawcą oprogramowania i prawdopodobnie poniesienia określonych kosztów związanych z konieczną modyfikacją (zwracamy uwagę na przyjęte w rozporządzeniu rozwiązania, takie jak ***right-to-erasure*** czy ***privacy-by-design***). Jednocześnie większość przedsiębiorców jeszcze nie wie, czy planowane jest zwiększenie zasobów finansowych lub ludzkich na ochronę informacji.

Przedsiębiorcy planują natomiast podnoszenie poziomu świadomości i wiedzy personelu – zarówno poprzez wewnętrzne kanały komunikacji, jak i na przykład przez wysłanie pracownika na studia podyplomowe w zakresie ochrony danych osobowych.

Kluczowe czynniki

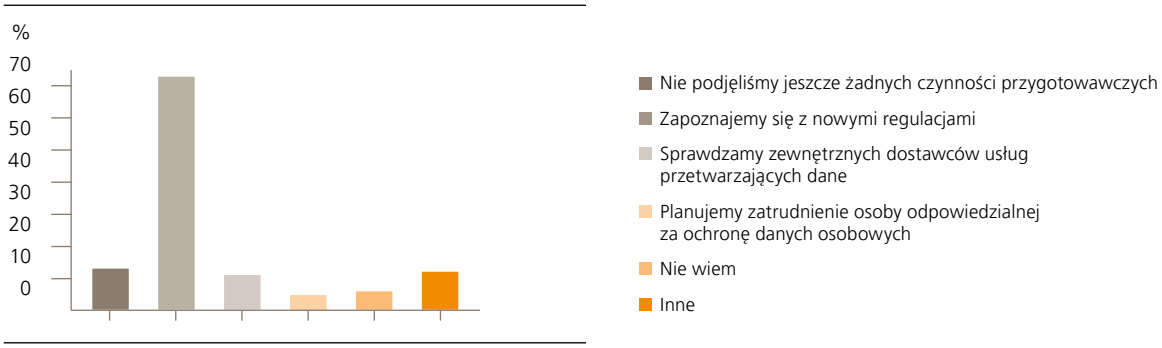
Zaangażowanie zarządu w proces wdrożenia nowych przepisów unijnych jest zjawiskiem wysoce pożądanym – choćby ze względu na wagę nowych obowiązków i potencjalne sankcje. Zarząd powinien być poinformowany o nadchodzących zmianach i włączony w działania na wczesnym etapie, aby mieć wpływ na kształtowanie kultury organizacyjnej firmy w zakresie ochrony danych osobowych.

Podobnie należy oceniać angażowanie podmiotów zewnętrznych, które profesjonalnie zajmują się dostosowywaniem prowadzonej działalności do nowego prawa. Włączenie ich w proces zmian pozwala korzystać z cudzych doświadczeń i unikać błędów popełnionych przez innych.

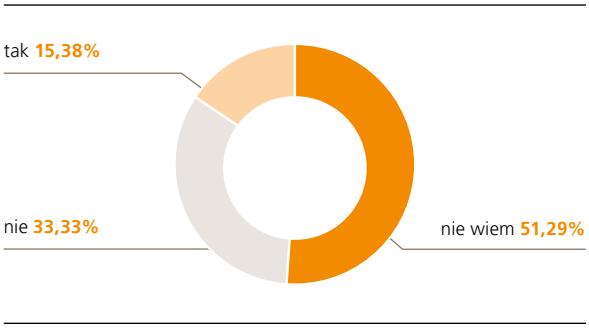
Przygotowujemy odpowiednie procedury i polityki pozwalające na sprawne reagowanie na naruszenia.

uczestnik badania CMS

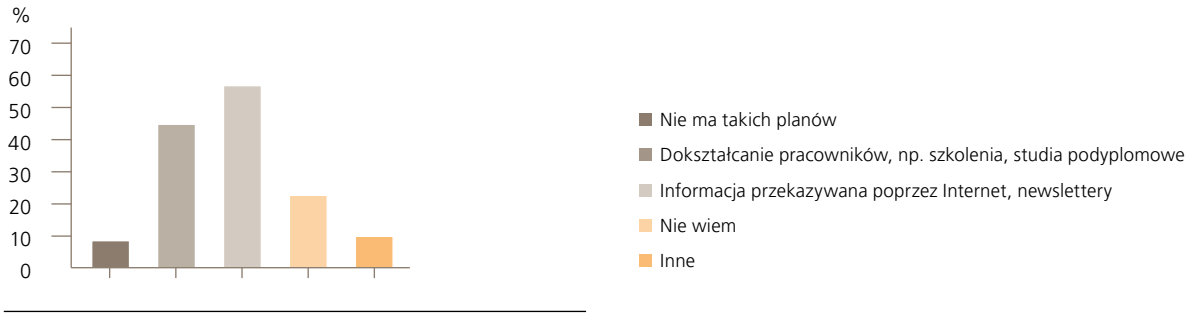
Jakie czynności przygotowawcze w celu dostosowania prowadzonej działalności do wymogów nowego prawa podjęła dotychczas Pani/Pana firma?



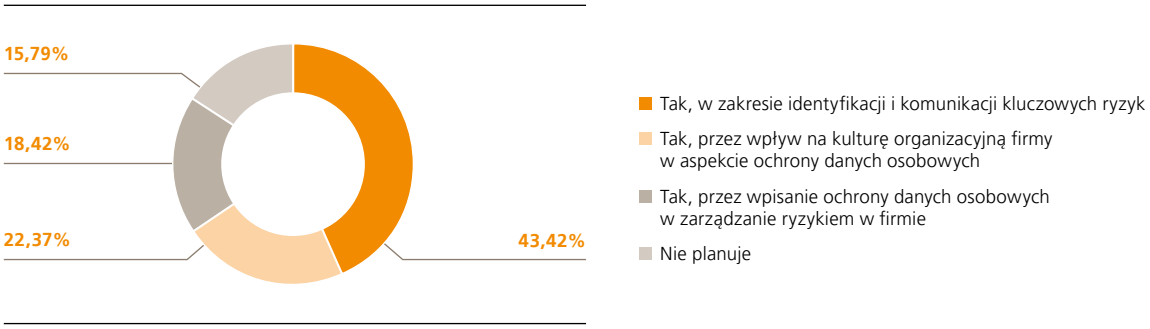
Czy Pani/Pana firma planuje zwiększenie zasobów (finansowych i/lub ludzkich) na ochronę informacji, w tym danych osobowych, w związku z nowym prawem?



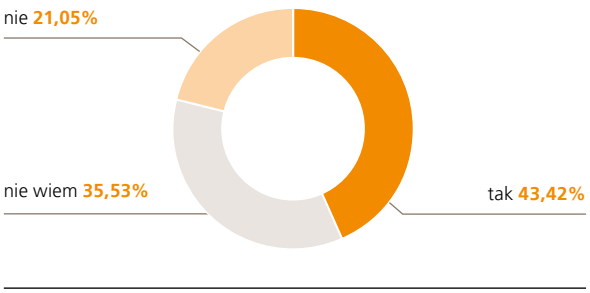
Czy i w jaki sposób Pani/Pana firma planuje zwiększenie świadomości pracowników co do nowego prawa?



Czy Pani/Pana firma planuje włączenie zarządu we wdrożenie nowych europejskich regulacji dotyczących ochrony danych osobowych?



Czy wdrażając nowe prawo ochrony danych osobowych, Pani/Pana firma zamierza skorzystać z ekspertyzy i doświadczeń zewnętrznych dostawców usług?



IV. Postrzeganie sytuacji

Większość ankietowanych przedsiębiorców widzi potrzebę dalszego informowania o nadchodzących zmianach.

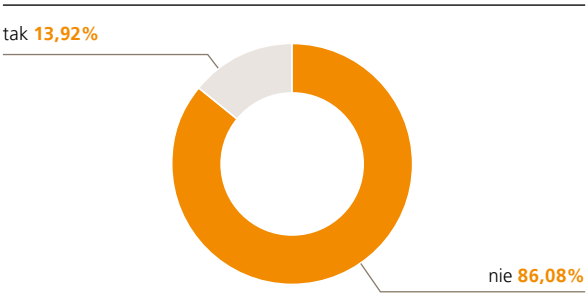
Zarówno Generalny Inspektor Ochrony Danych Osobowych (GIODO), jak i inne podmioty podejmowały działania edukacyjne w zakresie zmian. Mimo to, poziom wiedzy przedsiębiorców nadal pozostawia wiele do życzenia. Być może zaistniała sytuacja wynika z faktu, że równocześnie z pracami nad unijnym rozporządzeniem w Polsce prowadzono prace nad zmianami do ustawy o ochronie danych osobowych, na przykład w związku z pełnieniem funkcji administratora bezpieczeństwa informacji. Należy mieć nadzieję, że w niedalekiej przyszłości będzie prowadzona intensywniejsza edukacja.

Zgodność się opłaca

Przedsiębiorcy są w znakomitej większości zgodni co do tego, dlaczego warto przestrzegać nowych przepisów: przede wszystkim ze względu na ryzyko finansowe i możliwe sankcje, jak też ryzyko reputacyjne.

Z drugiej strony, jedynie połowa z nich uważa, że klienci oczekują poszanowania swojej prywatności. W naszej ocenie ta sytuacja będzie się zmieniać głównie dlatego, że coraz więcej przedsiębiorstw będzie działać w oparciu o skomplikowane metody przetwarzania danych i wyciągania z nich odpowiednich wniosków. Dane są walutą cyfrowego świata i ich strata może okazać się dla biznesu bardzo dotkliwa.

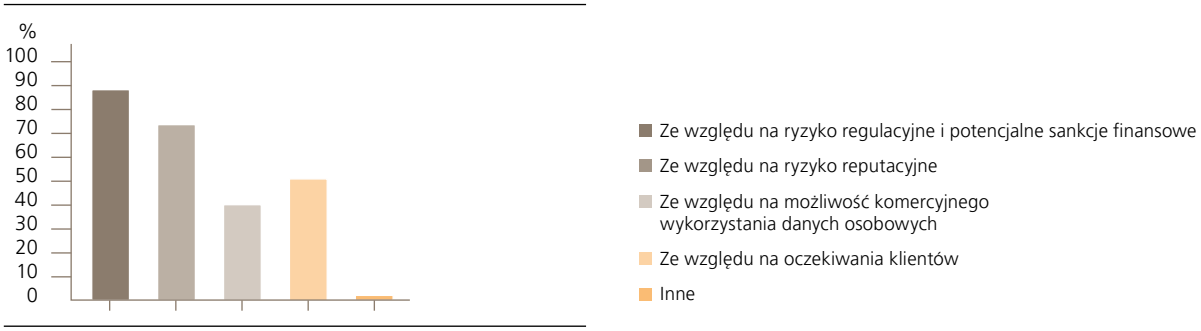
Czy Pani/Pana zdaniem, przedsiębiorcy są właściwie informowani o nadchodzących zmianach?



Będziemy prowadzić działalność edukacyjno-informacyjną, by pomóc podmiotom zobowiązanym w dostosowaniu się do nowych zasad przetwarzania danych osobowych określonych w unijnym rozporządzeniu.

dr Edyta Bielak-Jomaa, GIODO

Dlaczego Pani/Pana zdaniem warto przestrzegać nowych europejskich przepisów o ochronie danych osobowych?



Ochrona danych osobowych 2.0

Nowe unijne rozporządzenie zmieniające zasady ochrony danych osobowych weszło w życie 25 maja 2016 r.

Nowe prawo jest wspólne i – co do zasady – jednolite dla całej Unii Europejskiej. Dla polskiego systemu ochrony danych oznacza to, że to obszerne rozporządzenie zastąpi obecnie obowiązującą ustawę o ochronie danych osobowych prawdopodobnie w całości.

Co więcej – i jest to nowość warta uwagi – unijna regulacja obejmie nie tylko przedsiębiorstwa z Unii Europejskiej, ale również te, które swoją siedzibę mają poza jej granicami, choć oferują obywatelom Unii swoje towary bądź usługi lub też monitorują ich zachowania.

Zyskują konsumenci

Nowe przepisy znacznie wzmacniają prawa osób fizycznych, których dotyczą dane osobowe. Nie zakazują czerpania korzyści z przetwarzania danych klientów, formułują jednak określone reguły postępowania i wynikające z nich obowiązki, tak by cały proces przetwarzania danych był transparentny.
W praktyce oznacza to, że czasy, w których kwestia ochrony danych osobowych była przez niektórych traktowana z przymrużeniem oka, odchodzą bezpowrotnie w przeszłość. To, co jeszcze niedawno było dobrą praktyką, stanie się obligatoryjnym standardem funkcjonowania dla polskich przedsiębiorców.

Więcej obowiązków dla firm

Postawienie na przejrzystość przetwarzania danych i realne informowanie osób o gromadzeniu i wykorzystywaniu ich danych będzie sporym wyzwaniem dla wielu firm. Przedsiębiorca będzie musiał zadbać o to, by wszelkie informacje i komunikaty związane z przetwarzaniem danych były łatwo dostępne, zrozumiałe oraz sformułowane jasnym i prostym językiem.

> Regulacja obejmuje wszystkie przedsiębiorstwa z Unii Europejskiej i podmioty spoza jej granic, oferujące obywatelom Unii swoje towary bądź usługi lub też monitorujące ich zachowania.

Jednocześnie zwiększeniu ulegnie zakres informacji przekazywanych osobom przez administratora danych osobowych. Wśród nich znajdą się na przykład informacje o profilowaniu, prawie do przenoszenia danych do innego dostawcy usług, prawie do cofnięcia zgody czy też informacje o okresie przechowywania danych osobowych.

Tylko bezpieczni podwykonawcy

W porównaniu z obecnie obowiązującą ustawą, nowe unijne prawo wymaga znacznie większej odpowiedzialności i świadomości przy przetwarzaniu danych osobowych. I to zarówno ze strony administratorów danych, jak i podmiotów przetwarzających dane na zlecenie.

Administratorzy danych będą mogli zawierać umowy o powierzenie przetwarzania danych tylko z takimi podmiotami, które gwarantują właściwe wdrożenie przepisów rozporządzenia, m.in. stosują środki bezpieczeństwa adekwatne do ryzyka związanego z przetwarzaniem i regularnie monitorują skuteczność zasobów technicznych oraz organizacyjnych, mających zapewnić bezpieczeństwo.

ABI 2.0 czyli inspektor ochrony danych

Nowa regulacja znacznie zmienia rolę administratora bezpieczeństwa informacji. Według rozporządzenia zastąpi go inspektor ochrony danych. Jeden inspektor będzie mógł działać w więcej niż jednym przedsiębiorstwie tylko wówczas, gdy każda z tych firm będzie mogła łatwo nawiązać z nim kontakt. To powinno usprawnić funkcjonowanie grup kapitałowych, które koordynują działania zmierzające do ochrony danych.

Katalog zadań inspektora został ujednolicony w skali całej Unii Europejskiej. Do jego obowiązków będzie należeć m.in. monitorowanie przestrzegania rozporządzenia poprzez działania i szkolenia pracowników danej spółki, jak również współpraca z Generalnym Inspektorem Ochrony Danych Osobowych (GIODO).

> Kary będą bardzo dotkliwe – nawet 20 mln euro lub 4% globalnego rocznego obrotu z poprzedniego roku finansowego.

Surowe sankcje

Unijny ustawodawca daje państwom członkowskim, organom ochrony danych osobowym i przedsiębiorstwom dwa lata na pełne dostosowanie się do nowych wymogów. Rozporządzenie będzie egzekwowane od 25 maja 2018 r.

By zapewnić przestrzeganie przepisów rozporządzenia, unijny ustawodawca nie zawahał się wprowadzić surowych sankcji. Nowa regulacja umożliwia nakładanie kar finansowych w prawie 30 przypadkach, na przykład w przypadku niedochowania obowiązków związanych z warunkami uzyskania zgody na przetwarzanie danych czy niedoinformowania organu nadzoru o wycieku danych.

Kary mogą być dla przedsiębiorców bardzo dotkliwe – nawet 20 mln euro lub 4% globalnego rocznego obrotu w poprzednim roku finansowym (w zależności od tego która z tych kwot jest wyższa).

Konsekwencje dla biznesu

Wszyscy przedsiębiorcy działający w Polsce będą musieli prowadzić swoją działalność w zgodzie z nowym unijnym prawem dotyczącym ochrony danych osobowych.

Oto przykłady wyzwań, jakie rozporządzenie stawia przed biznesem w zakresie ochrony danych osobowych:

Transparentność – zasada przejrzystości

Wszystkie osoby, których dane przetwarzane są przez firmę, na przykład pracownicy czy klienci, muszą być w znacznie szerszym zakresie niż dotychczas informowane o tym, co się dzieje z ich danymi. Przedsiębiorcy będą musieli zadbać o przejrzystość, rzetelność i czytelność tych informacji.

Rzetelny wybór podmiotu przetwarzającego dane osobowe (tzw. procesora)

To przedsiębiorcy będą odpowiedzialni za ocenę, czy wybrany dostawca usługi przetwarzania danych dysponuje koniecznymi w tym celu środkami technicznymi i organizacyjnymi. Już dziś warto więc pomyśleć o implementacji nowej procedury wyboru dostawcy lub też dostosowaniu obecnie istniejącej do bardziej wymagającego otoczenia prawnego.

Profilowanie klientów

Zmiany w zakresie zautomatyzowanego przetwarzania danych osobowych to jeden z kluczowych dla prowadzenia biznesu elementów unijnego rozporządzenia. Nowe prawo dopuszcza profilowanie oparte na automatycznym przetwarzaniu danych dopiero po uzyskaniu zgody zainteresowanego, chyba że profilowanie jest konieczne do zawarcia lub wykonania umowy. Regulacja nakazuje informowanie konsumentów o tym, że podlegają oni profilowaniu. Przedsiębiorcy będą musieli wdrożyć odpowiednie mechanizmy, by zagwarantować osobom fizycznym ich prawa związane z profilowaniem, w szczególności prawo do sprzeciwu wobec decyzji opartej na profilowaniu.

Bezpieczeństwo danych

Rozporządzenie wiele miejsca poświęca kwestii bezpieczeństwa danych osobowych. Nowe przepisy wymagają od przedsiębiorców, by o wszystkich przypadkach naruszenia danych informowali Generalnego Inspektora Ochrony Danych Osobowych (GIODO), a niekiedy także zainteresowane osoby (np. klientów), których dane dotyczą. Wszelkie nieprawidłowości w tym zakresie należy zgłosić organowi nadzorczemu (GIODO) bez zbędnej zwłoki, jeżeli to możliwe – nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia. Dotyczy to nie tylko takich przypadków, gdy dane zostaną na przykład bezprawnie opublikowane w Internecie, ale też sytuacji, kiedy zgubiony zostanie pendrive z danymi czy dane zostaną skasowane.

Inspektor ochrony danych *(Data Protection Officer)*

Zgodnie z rozporządzeniem, powołanie inspektora ochrony danych w sektorze prywatnym będzie obowiązkowe w dwóch przypadkach: kiedy przetwarzanie danych ze względu na ich charakter, naturę, cel lub zakres wymaga regularnego i systematycznego monitorowania osób na dużą skalę, a także gdy na dużą skalę przetwarzane są dane szczególnej kategorii (dane wrażliwe) lub dane osobowe dotyczące wyroków skazujących. W pozostałych przypadkach powołanie inspektora ochrony danych będzie dobrowolne.

Jak dostosować się do nowych przepisów?

Dla wielu przedsiębiorców dostosowanie prowadzonej działalności do nowego prawa w tak krótkim czasie, czyli do 25 maja 2018 r., będzie dużym wyzwaniem.

Zapewnienie środków technicznych, organizacyjnych i finansowych koniecznych do funkcjonowania w zgodzie z nowymi wymogami może okazać się procesem długotrwałym, żmudnym i – w większości przypadków – kosztownym.

Zacznij już teraz

Rekomendujemy, by niezbędne prace wdrożeniowe zacząć jak najszybciej. Tylko niezwłoczna i trafna identyfikacja potencjalnych ryzyk związanych z przetwarzaniem danych pozwoli zareagować na nie skutecznie i z odpowiednim wyprzedzeniem. W tym celu niezbędna jest precyzyjna analiza procesów biznesowych i zestawienie ich z wymogami nowej regulacji.

Zaangażuj zespół

Sugerujemy stworzenie specjalnej grupy roboczej, która będzie odpowiadać za wdrożenie zmian i dostosowanie spółki do nowych przepisów. Grupa powinna składać się z osoby odpowiadającej za ochronę danych osobowych i przedstawicieli wszystkich tych jednostek organizacyjnych, na które największy wpływ będzie miało nowe prawo. Taka szeroka reprezentacja da pewność, że zmiany będą uwzględniać ochronę danych osobowych we wszystkich biznesowo istotnych obszarach funkcjonowania przedsiębiorstwa.

Zaplanuj pracę

Niezbędne jest szczegółowe rozpisanie planu działań w czasie. Z jednej strony powinien on uwzględniać wagę poszczególnych zadań do zrealizowania, z drugiej wysiłek organizacyjny, jaki potrzebny jest do wprowadzenia danej zmiany.

Plan powinien wskazywać konkretne osoby odpowiedzialne za wdrożenie i uwzględniać priorytety, jak też czas, którym dysponuje przedsiębiorstwo na wdrożenie. Warto również pamiętać, że część pracy będzie musiała być wykonana wewnątrz firmy, jednak część wymagać będzie współpracy z partnerami zewnętrznymi – dostawcami lub klientami.

10 kroków do zgodności

1. Przeprowadzenie analizy, czy powołanie inspektora ochrony danych dla całej grupy lub jej części w Polsce jest obligatoryjne, czy tylko wskazane ze względu na naturę przetwarzanych danych.

2. Stworzenie schematu przepływu danych do organizacji, wewnątrz niej i na zewnątrz; zdefiniowanie źródeł pozyskiwania danych, sposobu ich zbierania; określenie podmiotów, z którymi dane są dzielone; identyfikacja ryzyk związanych z tymi procesami.

3. Przeprowadzenie analizy dokumentacji wewnętrznej związanej z ochroną danych osobowych i stworzenie – wszędzie tam, gdzie jest to możliwe – zestandaryzowanego zbioru wzorów dokumentów dla wszystkich jednostek organizacyjnych przedsiębiorstwa oraz jego oddziałów.

4. Przeprowadzenie analizy oprogramowania pod kątem bezpieczeństwa danych osobowych i wymagań rozporządzenia, zwłaszcza w kontekście prawa do „bycia zapomnianym" *(Right to be Forgotten)* oraz prywatności w fazie projektowania *(Privacy by Design).*

5. Przeprowadzenie analizy potencjalnego ryzyka naruszenia danych osobowych *(Data Breach)* i możliwości ubezpieczenia się od tego ryzyka na polskim/unijnym rynku ubezpieczeniowym.

6. Stworzenie i wdrożenie na stałe w spółce procesu oceny wpływu nowych przedsięwzięć związanych z przetwarzaniem danych osobowych na ochronę prywatności *(Privacy Impact Assessment).*

7. Zwiększenie świadomości wymagań, jakie stawia przed organizacją rozporządzenie wśród jej pracowników, partnerów i klientów.

8. Weryfikacja dostawców usług dla firmy pod kątem ich zdolności do skutecznej ochrony danych osobowych zgodnej z przepisami nowego rozporządzenia.

9. Renegocjowanie umów powierzenia, które – zgodnie z nowym prawem – muszą mieć bardzo rozbudowaną treść.

10. Spełnienie obowiązku informacyjnego wynikającego z nowej regulacji.

Racjonalne podejście

Rozmowa z Generalnym Inspektorem Ochrony Danych Osobowych, dr Edytą Bielak-Jomaa

foto: materiały GIODO

Rozporządzenie zachęca przedsiębiorców do tworzenia i przystępowania do branżowych kodeksów dobrych praktyk. Jak na to zapatruje się Generalny Inspektor Ochrony Danych Osobowych? Czy w ocenie organu samoregulacja branżowa może pozytywnie wpłynąć na poziom ochrony danych?

Uważam, że tzw. kodeksy dobrych praktyk, będące swego rodzaju zbiorem zasad, norm postępowania dotyczących przetwarzania danych osobowych, to rozwiązanie sprzyjające podnoszeniu poziomu ochrony danych osobowych. Idea ich tworzenia nie jest zresztą nowa, została bowiem ustanowiona w art. 27 Dyrektywy 95/46/WE Parlamentu Europejskiego, a Generalny Inspektor Ochrony Danych Osobowych od dawna inicjował i wspierał ich opracowywanie.

W rozporządzeniu tworzenie i zatwierdzanie kodeksów postępowania, bo taką nazwę im teraz nadano, jest znacznie bardziej precyzyjnie uregulowane i sformalizowane. Przewiduje między innymi zatwierdzanie i publikację kodeksów przez organ ds. ochrony danych osobowych, a także wprowadza mechanizm monitorowania przestrzegania przepisów tych dokumentów przez akredytowane przez GIODO podmioty dysponujące odpowiednim poziomem wiedzy fachowej w dziedzinie, której kodeks dotyczy. Nie zmienia to jednak samej istoty i celu ich powstawania, którym jest między innymi upowszechnianie oraz zunifikowanie podstawowych zasad przetwarzania danych osobowych i poprawnego ich zastosowania w praktyce.

Podkreślić jednak należy, że opracowanie i stosowanie kodeksu jako instrumentu pozwalającego na wykazanie, że administrator danych lub przetwarzający odpowiednio wdrożyli gwarancję ochrony danych osobowych, jest domniemaniem wzruszalnym, gdyż ani zatwierdzenie kodeksu przez GIODO, ani jego monitorowanie przez akredytowany podmiot nie wyłączy uprawnień kontrolnych organu ds. ochrony danych osobowych.

Jednym z obowiązków nałożonych na przedsiębiorców na gruncie rozporządzenia będzie przeprowadzanie tzw. oceny skutków dla ochrony danych (Privacy Impact Assessment), połączone z instytucją uprzednich konsultacji z organem ochrony danych. Czy w ocenie GIODO przedsiębiorcy działający w Polsce będą często korzystać z tej formy dialogu z regulatorem?

Biorąc pod uwagę to, jak wiele pytań z prośbą o interpretację przepisów prawa w kontekście stosowanych lub planowanych przez danego administratora danych rozwiązań wpływało w ostatnich latach do Biura GIODO, myślę, że przedsiębiorcy chętnie będą korzystać z przewidywanej przez unijne rozporządzenie możliwości konsultacji z organem ds. ochrony danych osobowych. Będą bowiem traktować je jak swego rodzaju zabezpieczenie, gwarancję, że wdrożone mechanizmy są zgodne z prawem i że w razie kontroli GIODO uzyskają ponowną akceptację. Trzeba jednak podkreślić, że nie każdy będzie mógł skorzystać z takiej formy współpracy z GIODO. Przepisy rozporządzenia ograniczają bowiem krąg uprawnionych do tego podmiotów.

Po pierwsze, do przeprowadzania oceny ryzyka i skutków wpływu projektu na prywatność oraz poziom ochrony danych administrator danych lub podmiot przetwarzający zobowiązany będzie wówczas, gdy operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów.

Po drugie zaś, jak stanowi art. 36, jeżeli ocena skutków planowanych operacji przetwarzania dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. Ponadto prawo państwa członkowskiego może wymagać, by administratorzy konsultowali się z organem nadzorczym i uzyskiwali jego uprzednią zgodę na przetwarzanie przez nich danych osobowych do celów wykonywanych w interesie publicznym zadań, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym. Rozporządzenie przewiduje też, że z organem nadzorczym konsultują się państwa członkowskie, przygotowując projekt aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania.

Rozporządzenie przewiduje wysokie sankcje finansowe w przypadku przetwarzania danych osobowych niezgodnie z prawem. Ankietowani uważają, że jest to jeden z decydujących czynników skłaniających ich do zgodnego z prawem przetwarzania danych. Czy w ocenie Generalnego Inspektora tak wysokie kary przyczynią się do podniesienia poziomu ochrony danych?

Rozporządzenie wprowadza zupełnie nowe spojrzenie na pozycję administratora danych i na niego przenosi ciężar odpowiedzialności za przetwarzanie danych osobowych niezgodnie z prawem. I to jest racjonalne podejście, bo to administrator wie, a przynajmniej powinien wiedzieć, jakie środki ma podjąć, by zapewnić bezpieczeństwo przetwarzanych przez siebie danych.

Konsekwencją tego nowego podejścia są przewidywane sankcje. Ich górna wysokość to 20 milionów euro, a w przypadku przedsiębiorstw – 4% rocznych globalnych obrotów z poprzedniego roku obrotowego. Z samego założenia kary te mają być skuteczne, proporcjonalne i odstraszające. I takie, jak sądzę, są. W mojej ocenie świadomość, że można zapłacić bardzo wysoką karę za niewłaściwe przetwarzanie danych, będzie mobilizowała do większej dbałości o nie i myślę, że to się dobrze sprawdzi.

Przedsiębiorcy mają aż lub tylko dwa lata na dostosowanie prowadzonej działalności do nowych przepisów. Czy w ocenie GIODO taki czas jest wystarczający? Co, zdaniem organu, powinni w pierwszej kolejności zrobić przedsiębiorcy, aby dobrze przepracować okres dostosowawczy?

Choć rozporządzenie zacznie bezpośrednio obowiązywać dopiero od 25 maja 2018 r., to już teraz warto zapoznać się z jego przepisami i rozpocząć przygotowania do jego stosowania we własnej firmie. Wbrew pozorom czasu nie jest aż tak dużo. A od czego zacząć? Moim zdaniem najważniejsza jest ocena własnej sytuacji, przegląd tego, jakie dane są przetwarzane, i określenie celu tego przetwarzania. Rozporządzenie wprowadza bowiem nowe kategorie danych, na przykład dane biometryczne, które dotychczas nie były zdefiniowane. Warto też zastanowić się nad oceną ryzyka związanego chociażby z wyciekiem danych. Tylko w ten sposób można wprowadzić skuteczne zabezpieczenia zarówno organizacyjne, jak i techniczne. Bez wątpienia rozporządzenie zwiększa zakres odpowiedzialności administratora danych za bezpieczeństwo danych osobowych, dlatego to w dobrze rozumianym interesie przedsiębiorcy jest o nie zadbać.

Czy Biuro GIODO planuje prowadzenie akcji informacyjnych, na przykład konferencji lub seminariów, poświęconych nowemu rozporządzeniu albo przygotowanie w tym zakresie materiałów informacyjnych dla przedsiębiorców?

Biuro GIODO takie działania edukacyjne zaczęło prowadzić już od momentu rozpoczęcia prac nad unijnym rozporządzeniem, informując o kolejnych ich etapach. Również były one przedmiotem dyskusji i debat podczas konferencji naukowych organizowanych przez GIODO, jak i inne, współpracujące z Urzędem podmioty. Także strona internetowa Generalnego Inspektora była i jest źródłem wiedzy o zmianach, jakie wiążą się z unijnymi przepisami. Nadal więc będziemy prowadzić tę działalność edukacyjno-informacyjną, by pomóc podmiotom zobowiązanym w dostosowaniu się do nowych zasad przetwarzania danych osobowych określonych w unijnym rozporządzeniu. Wywodzę się ze środowiska naukowego, toteż kwestia edukacji jest dla mnie bardzo ważna i na pewno będę kontynuować dotychczasowe działania w tym obszarze.

O CMS

CMS jest międzynarodową kancelarią prawniczą świadczącą kompleksowe usługi doradztwa prawnego i podatkowego na rzecz przedsiębiorstw, instytucji finansowych oraz organów administracji. Jest jedną z największych i najbardziej doświadczonych międzynarodowych kancelarii w Polsce – działa na polskim rynku od ponad 20 lat. W biurze CMS w Warszawie pracuje 140 prawników, którzy doradzają klientom funkcjonującym we wszystkich kluczowych sektorach gospodarki.

Prawnicy CMS mają bogate doświadczenie we wszelkich aspektach prawnych dotyczących ochrony danych osobowych. Obejmuje ono między innymi doradztwo strategiczne w kwestiach przetwarzania danych osobowych przez największych administratorów danych w Polsce i Unii Europejskiej, kompleksowe audyty zgodności przetwarzania danych osobowych z prawem, jak też doradztwo w zakresie procesów przekazywania danych poza Europejski Obszar Gospodarczy, w tym kwestii wiążących reguł korporacyjnych (BCR). Wielokrotnie reprezentowali klientów w postępowaniach prowadzonych przez GIODO.

C/M/S/ Law-Now™

Law . Tax

www.cms-lawnow.com

C/M/S/ e-guides

Law . Tax

eguides.cmslegal.com

CMS Cameron McKenna Greszta i Sawicki sp. k. jest członkiem CMS Legal Services European Economic Interest Grouping (CMS EEIG), Europejskiego Zgrupowania Interesów Gospodarczych, które koordynuje działalność organizacji skupiającej niezależne kancelarie prawne. CMS EEIG nie świadczy usług doradczych, świadczą je wyłącznie kancelarie członkowskie CMS EEIG w ramach swoich jurysdykcji. CMS EEIG oraz każda z kancelarii członkowskich stanowią samodzielne i odrębne pod względem prawnym podmioty, z których żaden nie posiada uprawnień do zaciągania zobowiązań w imieniu pozostałych. CMS EEIG oraz każda z kancelarii członkowskich ponoszą odpowiedzialność wyłącznie za swoje własne działania i zaniechania. Nazwa „CMS" oraz określenie „kancelaria" odnoszą się do niektórych bądź do wszystkich kancelarii członkowskich lub ich poszczególnych biur.

Biura CMS:
Aberdeen, Algier, Amsterdam, Antwerpia, Barcelona, Belgrad, Berlin, Bratysława, Bristol, Bruksela, Budapeszt, Bukareszt, Casablanca, Dubaj, Düsseldorf, Edynburg, Frankfurt, Genewa, Glasgow, Hamburg, Stambuł, Kijów, Kolonia, Lipsk, Lizbona, Lublana, Londyn, Luksemburg, Lyon, Madryt, Maskat, Mediolan, Meksyk, Monachium, Moskwa, Paryż, Pekin, Podgorica, Praga, Rio de Janeiro, Rzym, Sarajewo, Sewilla, Sofia, Strasburg, Stuttgart, Szanghaj, Teheran, Tirana, Utrecht, Warszawa, Wiedeń, Zagrzeb, Zurych.

---

cmslegal.com