Ogólne rozporządzenie o ochronie danych (RODO):

Skrócony podręcznik Sage dla firm

Spis treści

Wprowadzenie

Ogólne rozporządzenie o ochronie danych (RODO) stanowi nowe ramy prawne, które z dniem 25 maja 2018 r. wejdą w życie w Unii Europejskiej („UE"). Rozporządzenia UE mają bezpośrednią skuteczność we wszystkich państwach członkowskich UE, co oznacza, że RODO będzie nadrzędne wobec wszelkich przepisów krajowych.

Celem RODO jest ochrona danych osobowych, tj. danych osób fizycznych. W rzeczywistości RODO to jedna z największych zmian w zakresie sposobu postępowania z danymi dotyczącymi osób fizycznych, która potencjalnie wpływa nie tylko na przedsiębiorstwa, ale również na wszystkie osoby fizyczne, korporacje, organy administracji publicznej lub inne podmioty mające w posiadaniu dane osobowe osób fizycznych z UE, w tym na dostawców i inne strony trzecie, z usług których przedsiębiorstwo może korzystać w zakresie przetwarzania danych osobowych.

Rozporządzenie ma zaskakująco szeroki zasięg. Obejmuje wszystkie państwa członkowskie Unii Europejskiej, w tym także Wielką Brytanię po Brexicie w 2019 r., ponieważ RODO zostanie włączone do prawodawstwa brytyjskiego. W przeciwieństwie do zasad dotyczących ochrony danych osobowych zawartych w Dyrektywie 95/46, RODO ma także wpływ na przedsiębiorstwa spoza UE oferujące towary lub usługi na rzecz osób fizycznych w UE lub monitorujące ich zachowanie na terenie UE. Ma ono na przykład bezpośredni wpływ na firmy hostingowe z USA, które świadczą usługi hostingu stron dostępnych dla osób fizycznych w UE.

Implikacje RODO są bardzo szerokie - właściwie można powiedzieć, że obejmują niemal każdy dział w przeważającej większości firm na całym świecie. Niektóre z nich mogą być na przykład zmuszone zatrudnić inspektora ochrony danych. Prawie wszystkie zaś będą musiały wprowadzić dodatkowe procedury i zabezpieczenia. Znajomość RODO należy uznać za bezwzględnie obowiązkową, gdyż jej brak może pociągać za sobą karę pieniężną w wysokości 4% rocznych globalnych obrotów lub 20 milionów euro, w zależności od tego, która z tych kwot będzie wyższa. W związku z tym zdecydowanie zaleca się przeprowadzenie audytu przez osobę posiadającą do tego stosowne kwalifikacje.

Niniejsza publikacja ma z założenia stanowić zwięzły, uproszczony podręcznik dla przedsiębiorstw. Więcej informacji można uzyskać od organów nadzorczych, takich jak Information Commissioner's Office (ICO) w Wielkiej Brytanii (w Polsce iest to Generalny Inspektor Ochrony Danych Osobowych - GIODO) oraz z wydanych przez nie publikacji „Overview of the General Data Protection Regulation". Prosimy zapoznać się z zastrzeżeniem prawnym Sage zawartym na końcu tej publikacji.

Infografika:

RODO w pigułce

Zgoda

Musi zostać potwierdzona w formie oświadczenia lub innej jednoznacznej czynności potwierdzającej. Nie można zakładać udzielenia zgody ani wykorzystywać domyślnie zaznaczonych pól na stronach internetowych.

Prawa jednostki

Znacznie rozszerza prawa jednostki oraz zakres informacji, jakie należy jej udostępnić w odniesieniu do przetwarzania danych.

Inspektor ochrony danych

Zatrudnienie go może być obowiązkowe. Musi on posiadać wiedzę specjalistyczną z zakresu przepisów o ochronie danych. Może być pracownikiem lub osobą zatrudnioną na podstawie umowy o świadczenie usług.

Sankcje

Mogą sięgać 4% rocznych globalnych obrotów lub 20 milionów EUR, w zależności od tego, która z tych kwot będzie wyższa. Kara pieniężna może zostać nałożona, nawet jeśli nie dojdzie do faktycznej utraty danych.

Ogólne rozporządzenie o ochronie danych (RODO)

Prywatność od początku do końca

Względy ochrony prywatności należy uwzględnić na każdym etapie działalności, a wykorzystywane mogą być wyłącznie dane ściśle wymagane do określonego celu.

Przenoszenie danych

Osoby fizyczne mają teraz prawo do przenoszenia, kopiowania lub przekazywania swoich danych osobowych – nawet do konkurencji.

Szerszy zakres

Obejmuje Twoją firmę oraz podmioty przetwarzające dane w Twoim imieniu – także spoza UE.

Obowiązek zgłaszania naruszeń

Administratorzy danych muszą powiadomić lokalne organy nadzorcze, takie jak GIODO, w ciągu 72 godzin od uzyskania informacji o naruszeniu. W przypadku poważnych naruszeń powiadomione muszą zostać też osoby fizyczne.

Podstawy

RODO przedstawia minimalne wymagania dotyczące postępowania z wszystkimi danymi osobowymi. Dane osobowe można zdefiniować jako wszelkie dane identyfikujące osobę fizyczną lub jej dotyczące (w tym, między innymi, cechy wyglądu fizycznego czy nawet dane biometryczne).

Większość przedsiębiorstw zbiera dane osobowe od chwili nawiązania interakcji z osobą fizyczną, niekiedy nawet nie zdając sobie z tego sprawy. Zbieranie danych osobowych może na przykład obejmować tak podstawowe czynności, jak wykorzystywanie plików cookie śledzących użytkowanie strony internetowej w celu identyfikacji użytkownika. Może także obejmować tak szczegółowe dane, jak rejestr osoby fizycznej w bazie danych oprogramowania do zarządzania relacjami z klientem („CRM"), a nawet jeszcze bardziej szczegółowe informacje. Dane osobowe mogą być zbierane lub przetwarzane dla wyłącznej korzyści osoby, której dotyczą, ale wciąż mają tu zastosowanie postanowienia RODO.

Podobnie jak Dyrektywa 95/46, RODO grupuje zasady dotyczące postpowania z danymi osobowymi w trzy zasadnicze zbiory: zasady dotyczące ochrony danych, zasady dotyczące przetwarzania danych zgodnie z prawem oraz zasady dotyczące ograniczenia międzynarodowego przekazywania danych. Choć większość przedsiębiorców i osób fizycznych prawdopodobnie zna już te zasady, zostały one bardziej szczegółowo opisane w niniejszym dokumencie. Warto się z nimi zapoznać, chociażby dla odświeżenia już posiadanych wiadomości.

RODO wprowadza też kilka ważnych nowych wymogów.

Podsumowanie postanowień RODO

Oto najważniejsze obszary regulowane przez RODO, ze szczególnym uwzględnieniem przepisów Dyrektywy 95/46 o ochronie danych osobowych.

Prawa jednostki oraz informowanie o nich

Obecnie obowiązujące w UE prawodawstwo w zakresie ochrony danych osobowych (Dyrektywa 95/46) daje osobom fizycznym prawo do dysponowania swoimi danymi osobowymi oraz opisuje, jakie informacje przedsiębiorstwa są zobowiązane przekazywać osobom fizycznym, które to infromacje obejmują między innymi wyjaśnienie zamiarów przedsiębiorcy w odniesieniu do danych osobowych. Dotychczas informacje i wyjaśnienia tego typu przyjmowały formę dostępnych na stronach internetowych oświadczeń lub powiadomień o ochronie prywatności.

RODO znacznie rozszerza ten wymóg, określając dodatkowe prawa, o których należy ponownie poinformować osoby fizyczne. W szczególności osoby fizyczne muszą zostać poinformowane o posiadaniu następujących praw (poniższy wykaz nie jest wyczerpujący):

1. do złożenia skargi do organów nadzorczych, takich jak ICO w Wielkiej Brytanii (w Polsce Generalny Inspektor Ochrony Danych Osobowych – GIODO);
2. do wycofania zgody na przetwarzanie swoich danych osobowych (patrz poniżej);
3. do uzyskania dostępu do swoich danych osobowych oraz ich sprostowania lub usunięcia („prawo do bycia zapomnianym") przez firmę, a także wszelkie strony trzecie, które uzyskały do nich dostęp;
4. do uzyskania informacji o istnieniu automatycznych systemów przetwarzania danych (w tym do profilowania);
5. do sprzeciwu wobec określonych rodzajów przetwarzania, np. do celów marketingu bezpośredniego lub decyzji opierających się wyłącznie na zautomatyzowanym przetwarzaniu;
6. do uzyskania informacji o tym, jak długo dane będą przechowywane;
7. do uzyskania informacji na temat wyznaczonego inspektora danych osobowych (patrz poniżej);

ponadto osoby fizyczne mają prawo do zwrócenia się do organizacji non-profit o wykonanie praw i wniesienie roszczeń w ich imieniu, na zasadach podobnych do pozwu zbiorowego w USA.

Zgoda

W przypadku gromadzenia danych na podstawie zgody osoby fizycznej, podczas gdy prawodawstwo UE w zakresie ochrony danych osobowych w odniesieniu do zbierania danych zawsze wymaga uzyskania dobrowolnej, świadomej zgody osoby fizycznej odnoszącej się do określonej sytuacji, na mocy RODO przedmiotowa zgoda musi zostać potwierdzona w formie oświadczenia lub innej jednoznacznej czynności potwierdzającej. Innymi słowy, domyślnie

zaznaczone pola na stronach internetowych lub milczenie/brak działania ze strony osoby fizycznej po zapoznaniu się z oświadczeniem o ochronie prywatności, nie będą jednoznaczne z wyrażeniem przez nią zgody.

Ponadto zgoda nie może mieć charakteru uniwersalnego, a więc firma nie może wykorzystać jednej zgody udzielonej przez osobę fizyczną na określonym etapie relacji biznesowych jako zgody na przetwarzanie danych osobowych w inny sposób lub w innym celu. Dla różnych operacji przetwarzania danych wymagane są osobne zgody.

Co więcej, osoba fizyczna nie tylko musi zostać poinformowana o przysługującym jej prawie do wycofania zgody w każdej chwili, ale wycofanie zgody musi być równie łatwe jak jej udzielenie.

W świetle RODO, dotychczasowe zgody udzielone przez osoby fizyczne muszą być przez firmy ponownie zweryfikowane w celu upenienia się, że spełniają one nowe wymogi. W razie sprzeczności lub niejednoznaczności przedsiębiorstwa będą musiały ustanowić nowe zgodne z prawem podstawy do przetwarzania danych (np. podstawą może być konieczność wykonania umowy), uzyskać nową zgodę lub zaprzestać przetwarzania danych osobowych.

Prawo do przekazywania danych osobowych (przenoszenie danych)

Osoby fizyczne mają teraz prawo do przenoszenia, kopiowania lub przekazywania swoich danych osobowych z jednego miejsca w drugie, nawet do konkurencji. Na przykład użytkownik korzystający z określonego serwisu muzycznego, który postanowi zacząć korzystać z oferty innego usługodawcy, może zabrać ze sobą listę odtwarzania generowaną przez pierwotny serwis muzyczny. W związku z tym dane osobowe muszą być przechowywane w uporządkowanym, powszechnie wykorzystywanym i nadającym się do odczytu maszynowego formacie, aby możliwe było ich łatwe wykorzystanie i udostępnienie.

Wymóg zapewnienia faktycznej możliwości przenoszenia danych i ich łatwego wykorzystywania przez innych może wiązać się z potrzebą wprowadzenia znacznych modyfikacji w zakresie infrastruktury informatycznej, a co za tym idzie, z kosztami.

O wiele szerszy zakres

Mówiąc najprościej, RODO nakłada odpowiedzialność za naruszenia nie tylko na przedsiębiorstwo zbierające dane, ale także na wszelkie zewnętrzne podmioty przetwarzające dane osobowe w jego imieniu, niezależnie od tego, czy będzie to inne przedsiębiorstwo, organizacja, czy osoba fizyczna. Nie oznacza to jednak, że firma może po prostu przekazać dane osobowe stronie trzeciej, a następnie przymykać oczy na nieprawidłowości. Przedsiębiorstwo jest zobowiązane dopilnować spełniania wymogów RDO również przez dostawcę zewnętrznego.

Zakres geograficzny RODO nie ogranicza się tylko do UE, obejmuje bowiem każde przedsiębiorstwo – i każdy zewnętrzny podmiot przetwarzający dane osobowe w jego imieniu – oferujące towary lub usługi na rzecz osób fizycznych w UE lub monitorujące zachowania osób w UE. W szczególności nie ma znaczenia odpłatność towarów lub usług, a zatem do spełniania wymogów RODO zobowiązane są również organizacje dobroczynne i pozarządowe.

W związku z tym, że UE jest partnerem handlowym większości krajów, rozszerzenie zakresu RODO ma konsekwencje dla wielu przedsiębiorstw na całym świecie. Przestrzeganie RODO wymagane jest od wszystkich przedsiębiorstw prowadzących działalność w państwach członkowskich UE niezależnie od tego, czy współpraca odbywa się bezpośrednio, czy w charakterze partnerów zewnętrznych innych firm.

Dowód wywiązywania się z obowiązku prawnego

Nie wystarczy tylko spełniać wymogi RODO. Zgodnie z wprowadzoną przez RODO zasadą „rozliczalności" przedsiębiorstwo musi być w stanie udowodnić przestrzeganie uregulowń RODO, co oznacza konieczność wypełniania pewnych dość uciążliwych wymogów dotyczących prowadzenia ewidencji. W szczególności należy dokumentować czynności przetwarzania*, wnioski o udostępnienie danych osoby, której dane dotyczą, naruszenia, sposób uzyskania zgody oraz oceny skutków dla ochrony danych (patrz poniżej).

Wymóg ten dotyczy również zewnętrznych podmiotów przetwarzających dane osobowe w imieniu przedsiębiorstwa, chociaż w tym przypadku wymogi nie są tak szczegółowe.

** Dotyczy przedsiębiorstw zatrudniających ponad 250 osób oraz przedsiębiorstw zatrudniających mniej niż 250 osób, w przypadku których przetwarzanie danych może wiąać się z ryzykiem naruszenia praw lub wolności osób fizycznych, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, takie jak informacje o stanie zdrowia, wyznaniu lub orientacji seksualnej.*

Prywatność od początku do końca

Techniczne i organizacyjne środki ochrony prywatności zgodne z oczekiwaniami danej osoby fizycznej muszą być stosowane przez cały okres życia danych osobowych – od początku czynności związanej z pozyskiwaniem danych, poprzez fazę ich wykorzystania, aż do zakończenia czynności, do której dane były potrzebne. Proces ten nazywany jest „ochroną prywatności w fazie projektowania" (privacy by design) i polega na uwzględnieniu kwestii dotyczących ochrony prywatności na każdym etapie procesu opracowywania, począwszy od fazy projektowania.

Ponadto faktycznie przetwarzane powinny być tylko konkretnie wymagane dane osobowe, które są ściśle wymagane – co określa się mianem zasady minimalizacji danych lub „domyślną ochroną prywatności" (Privacy by Default).

W praktyce przestrzeganie zasady ochrony prywatności w fazie projektowania oraz domyślnej ochrony danych będzie wiązać się z potrzebą ciągłego szkolenia, regularnego przeprowadzenia audytów, ograniczenia do minimum zbieranych danych, ograniczenia dostępu do danych osobowych na zasadzie „koniecznej potrzeby" oraz wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa, takich jak pseudonimizacja i szyfrowanie.

Obowiązek zgłaszania naruszeń

W przypadku naruszenia RODO firmy zbierające dane osobowe są zobowiązane do poinformowania o tym organów nadzorczych – takich jak ICO w Wielkiej Brytanii (w Polsce – Generalny Inspektor Ochrony Danych Osobowych) w ciągu 72 godzin od uzyskania informacji o takim naruszeniu. Zewnętrzne podmioty przetwarzające dane osobowe w imieniu danej firmy są zobowiązane do powiadomienia jej bez zbędnej zwłoki.

Jeśli naruszenie stwarza duże zagrożenie dla osób zainteresowanych, przedsiębiorstwa muszą także bez zbędnej zwłoki poinformować o nim osoby, których dane dotyczą.

Inspektor ochrony danych (IOD)

Na mocy RODO przedsiębiorstwa i wszystkie zewnętrzne podmioty przetwarzające dane osobowe w ich imieniu są zobowiązane do wyznaczenia inspektora ochrony danych („IOD"), zawsze gdy: (i) są podmiotem publicznym; (ii) główna działalność przedsiębiorstwa lub zewnętrznego podmiotu przetwarzającego dane wymaga monitorowania osób fizycznych na dużą skalę; lub ich główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, w tym danych dotyczących wyroków skazujących i naruszeń prawa. IOD musi posiadać wiedzę specjalistyczną z zakresu przepisów dotyczących ochrony danych. Nie musi być on pracownikiem danego przedsiębiorstwa. Może to być osoba wykonująca zadania na podstawie umowy o świadczenie usług. Dane IOD należy przekazać organowi nadzorczemu, takiemu jak ICO w Wielkiej Brytanii (w Polsce – Generalny Inspektor Ochrony Danych Osobowych).

Sankcje

Za nieprzestrzegania RODO grożą surowe kary pieniężne, które mogą sięgać 4% rocznych globalnych obrotów lub 20 milionów EUR, w zależności od tego, która z tych kwot będzie wyższa. Kara pieniężna może zostać nałożona, nawet jeśli nie dojdzie do faktycznej utraty danych. Należy zwrócić uwagę na brak wyłączeń lub wyjątków dla małych przedsiębiorstw. Ponadto osoby fizyczne mają możliwość złożenia pozwu zbiorowego z wnioskiem o formalne zbadanie, spełniania wymogów RODO przez daną firmę.

Brexit

W 2017 r. w wyniku wyborów powszechnych w Wielkiej Brytanii na pięcioletnią kadencję wybrany został rząd konserwatywny. W tym okresie, a mianowicie w 2019 r., Wielka Brytania opuści Unię Europejską. Do tego czasu RODO będzie obowiązywać w Wielkiej Brytanii, podobnie jak we wszystkich państwach członkowskich UE. Jednak w wydanym po wyborach oświadczeniu na temat nowego prawodawstwa stwierdzono, że w kwestii nowych przepisów dotyczących ochrony danych

„wdrożone zostaną postanowienia Ogólnego rozporządzenia o ochronie danych i nowej Dyrektywy dotyczącej egzekwowania prawa z zakresu przetwarzania danych, wypełniając nasze zobowiązania w okresie pozostawania państwem członkowskim UE i pomagając Zjednoczonemu Królestwu zachować najlepszą pozycję w celu utrzymania zdolności wymiany danych z innymi państwami członkowskimi UE oraz w środowisku międzynarodowym po opuszczeniu UE".

Źródło: Przemówienie Królowej, czerwiec 2017

W związku z tym istnieje ewentualność, chociaż nie należy tego zakładać, że po opuszczeniu Unii Europejskiej Wielka Brytania będzie uznawana przez Komisję Europejską za kraj zapewniający „odpowiednią" ochronę, a więc mogą ją ominąć potencjalne problemy, np. zakaz przekazywania danych objętych ochroną. Zachęcamy do śledzenia tej strony w poszukiwaniu informacji na temat decyzji podejmowanych w przyszłości.

Nowe prawodawstwo Wielkiej Brytanii zastępuje ustawę o ochronie danych z 1998 r., której podstawą była Dyrektywa 95/46.

Podstawowe zasady RODO

Oprócz wyżej przedstawionych nowych wymogów, RODO – podobnie jak Dyrektywa 95/46 – zestawia zasady dotyczące postępowania z danymi osobowymi w trzy zasadnicze grupy:

- ***Zasady dotyczące ochrony danych:*** Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą. Muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne. Muszą być prawidłowe i w razie potrzeby aktualizowane. Należy podjąć wszelkie zasadne działania, aby nieprawidłowe dane osobowe zostały niezwłocznie usunięte lub sprostowane. Dane muszą być przechowywane w formie umożliwiającej identyfikację osoby fizycznej, przez okres nie dłuższy, niż jest to potrzebne oraz przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo – w tym ochronę przed nieuprawnionym lub niezgodnym z prawem dostępem oraz utratą, zniszczeniem lub uszkodzeniem.
- ***Zasady dotyczące przetwarzania danych zgodnie z prawem:*** Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z poniższych warunków: dana osoba fizyczna wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; przetwarzanie jest lub wkrótce będzie niezbędne do wykonania umowy, której stroną jest dana osoba fizyczna; przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego (np. złożenie dokumentacji podatkowej przez przedsiębiorstwo); przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub wymaganego przez organ publiczny; przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez przedsiębiorstwo (lub przez stronę trzecią) z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby fizycznej.
- ***Zasady dotyczące międzynarodowego przekazywania:*** RODO podtrzymuje ogólny zakaz przekazywania danych osobowych poza terytorium Europejskiego Obszaru Gospodarczego do krajów niezapewniających odpowiedniej ochrony. W momencie powstawania niniejszej publikacji kraje uznawane przez Komisję Europejską jako zapewniające „odpowiednią" ochronę to: Stany Zjednoczone w odniesieniu do firm dokonujących samodzielnej certyfikacji pod kątem spełniania warunków porozumienia pomiędzy Unią Europejską i Stanami Zjednoczonymi o ochronie prywatności danych (uwaga: nie oznacza to, że Stany Zjednoczone należą do krajów uznawanych za zapewniające odpowiednią ochronę), Andora, Argentyna, Guernsey, Izrael, Kanada (z ograniczeniem do Ustawy o ochronie danych osobowych i dokumentów elektronicznych (PIPEDA)), Nowa Zelandia, Szwajcaria, Urugwaj, Wyspa Jersey, Wyspa Man i Wyspy Owcze. W przypadku krajów, w stosunku do których brak decyzji o zapewnianiu odpowiedniej ochrony, przekazywanie danych jest ograniczone do określonych okoliczności, w tym gdy dokonywane jest na podstawie zgody, na w oparciu o standardowe klauzule umowne opublikowane przez Komisję Europejską albo w przypadku przekazywania danych wewnątrz firmy, z zastosowaniem wiążących reguł korporacyjnych.

Co można zrobić już teraz

- Odwiedź stronę ICO (brytyjski odpowiednik GIODO), która zawiera szereg wskazówek i informacji ogólnych. W szczególności zachęcamy do lektury wydanej przez ICO publikacji pt. „12 kroków przygowowujących do przestrzegania Ogólnego rozporządzenia o ochronie danych („Preparing for the General Data Protection Regulation – 12 steps to take now").
- Sprawdzić i dostosować swoje systemy zbierania i przetwarzania danych osobowych, aby zapewnić ich zgodność z RODO. Warto rozważyć przeprowadzenie audytu pod kątem zgodności z RODO, między innymi od strony prawnej i technicznej.
- Dopilnować zapoznania się przez pracowników i kontrahentów z wymogami RODO oraz zorganizować dla nich szkolenia w tym zakresie. Pamiętaj, że RODO czyni Cię odpowiedzialnym za podmioty zewnętrzne przetwarzające dane osobowe w Twoim imieniu.
- Zasięgnąć porady prawnej, aby lepiej zrozumieć implikacje RODO dla swojego przedsiębiorstwa.

Aby uzyskać więcej informacji, odwiedź: Sage.com/RODO

Zastrzeżenie prawne Sage

Wskazówki zawarte w niniejszym podręczniku mają charakter wyłącznie informacyjny. Nie należy ich traktować jako porady prawnej. Pragniemy podkreślić, że klienci niebędący pewni implikacji RODO dla swojego przedsiębiorstwa, powinni zasięgnąć porady prawnej we własnym zakresie.

Chociaż dołożyliśmy wszelkich starań, aby informacje opublikowane w tym podręczniku były poprawne i aktualne, Sage nie składa żadnych obietnic dotyczących ich kompletności lub dokładności; informacje są dostarczane w ich aktualnej postaci (*'as is'*), bez żadnych gwarancji, wyraźnych ani dorozumianych. Sage nie odpowiada za ewentualne błędy lub braki i nie będzie odpowiadać za żadne szkody (w tym, między innymi, za szkody z tytułu utraty możliwości wykonywania działalności gospodarczej lub utraty zysków) z tytułu odpowiedzialności umownej, deliktowej bądź innej w związku z wykorzystaniem tych informacji lub poleganiem na nich czy też w związku z podjęciem jakichkolwiek czynności lub decyzji w wyniku ich wykorzystania.