www.ksiegowanaswoim.pl

KNS
KSIĘGOWA NA SWOIM

RODO – biuro rachunkowe, na co zwrócić uwagę? cz. I

Paweł Skóra

18.07.2024

Czym jest RODO?

W Polsce przyjęło się określać sformułowaniem RODO:

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Prawo krajowe

Ustawa o ochronie danych osobowych z dnia 10 maja 2018r. tj. z dnia 30 sierpnia 2019r.
Ustawa m.in. określa :

- ✓ tryb zatwierdzania kodeksów postępowania dotyczącego ochrony przetwarzanych danych osobowych – do chwili obecnej nie ma opracowanego kodeksu postępowania dla biur ksiegowych,
- ✓ organ nadzorczy w sprawie ochrony danych osobowych – jest nim Prezes Urzędu Ochrony Danych Osobowych,
- ✓ jak postępować w przypadku naruszeń przepisów o ochronie danych osobowych,
- ✓ jak organ nadzorczy może kontrolować przestrzeganie przepisów o ochronie danych,
- ✓ odpowiedzialność cywilną za naruszenie o ochronie danych,
- ✓ odpowiedzialność karną za naruszenie przepisów o ochronie danych.

Prezes Urzędu Ochrony Danych Osobowych

W związku z naruszeniem przepisów o ochronie danych osobowych oraz w ramach kontroli przestrzegania przepisów PUODO może:

- Żądać tłumaczenia dokumentacji na język polski i to tłumaczenie organizacja wykonuje na własny koszt.
- Mieć dostęp do informacji objętych tajemnicą prawnie chronioną, przy czym podmiot może zastrzec informacje, dokumenty lub ich części zawierające tajemnicę przedsiębiorstwa, przedstawiane Prezesowi Urzędu. W takim przypadku Administrator lub podmiot przetwarzający jest obowiązany przedstawić Prezesowi Urzędu również wersję dokumentu niezawierającą informacji objętych zastrzeżeniem.
- Nałożyć karę grzywny od 500 do 5000 zł w przypadku niestawienia się wezwanego świadka lub biegłego w postępowaniu administracyjnym.
- Ograniczyć przetwarzanie danych osobowych, w przypadku uprawdopodobnienia, że przetwarzanie narusza przepisy o ochronie danych, może spowodować poważne i trudne do usunięcia skutki.
- Uznać, że przemawia za tym interes publiczny i po zakończeniu postępowania informuje o wydaniu decyzji na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.
- Może kontrolować zgodnie z zatwierdzonym planem kontroli,,
- Może kontrolować na podstawie uzyskanych informacji,
- Może kontrolować w ramach monitorowania przestrzegania przepisów rozporządzenia

Co to są „dane osobowe”

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; art. 4 RODO

Czym jest przetwarzanie danych osobowych

Przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie; Art. 4 RODO

Zasady dotyczące danych osobowych

Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (,,zgodność z prawem, rzetelność i przejrzystość'');

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (,,minimalizacja danych'');

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (,,prawidłowość'');

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (,,ograniczenie przechowywania'');

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (,,integralność i poufność'')

Czym jest biuro księgowe w rozumieniu RODO

Definicje podmiotów przetwarzające dane osobowe:

administrator - podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Administrator odgrywa największą rolę w procesach przetwarzania danych, gdyż to on decyduje o celu i sposobach przetwarzania danych.

Podmiot przetwarzający - który niekiedy jest zwany także procesorem – to podmiot, który przetwarza dane osobowe w imieniu administratora.

Najistotniejszą cechą podmiotu przetwarzającego jest to, że operacje przetwarzania danych wykonuje na zlecenia administratora i na jego rzecz i jest podmiotem zewnętrznym nieznajdujący się w strukturze organizacyjnej administratora.

Podmiot przetwarzający nie decyduje o celu i sposobach przetwarzania a realizuje cele wyznaczone mu przez administratora, który określa także sposoby przetwarzania danych.

Od podmiotu przetwarzającego należy odróżnić podmioty, które przetwarzają dane z upoważnienia administratora.

Mogą to być pracownicy zatrudnieni przy przetwarzaniu danych lub wykonujący czynności przetwarzania danych na podstawie umów cywilnoprawnych (np. umowy o dzieło lub zlecenia albo inne osoby (np. praktykanci), które administrator dopuścił do przetwarzania danych w ramach swojej struktury organizacyjnej.

Biuro rachunkowe jako podmiot przetwarzający (procesor)

Biuro rachunkowe w stosunkach z klientami jest najczęściej podmiotem przetwarzającym, ponieważ są mu powierzane przez klienta dane innych podmiotów/firm współpracujących w zakresie obsługi księgowo-kadrowej.

To ci klienci są administratorami danych, a powierzają do zewnętrznego biura rachunkowego dane czy to swoich pracowników, czy dotyczące transakcji, w celu realizacji odpowiednich usług księgowych.

Biuro rachunkowe jako administrator danych

W stosunkach dotyczących samej działalności biura księgowego dane swoich pracowników, współpracowników, kontrahentów, czy klientów biuro księgowe będzie administratorem danych

Księgowa jako podmiot działający z upoważnienia administratora

Księgowa/księgowy, która przychodzi do spółki w ramach umowy zlecenia i działa w ramach tej spółki jako „dział księgowo-kadrowy” będzie podmiotem działającym z upoważnienia administratora.

Wdrożenie RODO

W pierwszej kolejności powinniśmy zweryfikować, jakie kategorie danych osobowych znajdują się w naszym biurze księgowym.

Kategorie te to np. pracownicy, klienci, kontrahenci klientów, kandydaci, dostawcy.

To jest etap w którym powinniśmy już wiedzieć jakie dane osobowe są w biurze i w jakim celu je przetwarzamy.

Przetwarzanie danych

Zgodnie z artykułem 6 RODO przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Podstawa przetwarzania danych w biurze księgowym

Podstawą przetwarzania danych osobowych osób fizycznych np. w celach wystawienia faktur lub deklaracji jest:

- konieczność wykonania umowy, której stroną jest osoba fizyczna i zgoda tej osoby do przetwarzania danych (art. 6 ust. 1 lit.a i lit b RODO),

- uzasadniony interes przedsiębiorcy(biura księgowego) (art. 6 ust. 1 lit. f RODO).

Podstawa przetwarzania danych w biurze księgowym

Podstawą przetwarzania danych osobowych pracowników jest:

- konieczność wykonania umowy, której stroną jest pracownik (art. 6 ust. 1 lit. b),

- obowiązek prawny pracodawcy (art. 6 ust. 1 lit. c RODO),

- prawnie uzasadniony interes przedsiębiorcy (art. 6 ust. 1 lit. f RODO) lub

- zgoda pracownika (art. 6 ust. 1 lit. a RODO).

Biuro księgowe jako administrator jest zobowiązany w szczególności dopełnić wobec swoich kontrahentów obowiązków informacyjnych (art. 13-14 RODO).

Na przedsiębiorcy jako administratorze danych osobowych ww. osób ciążą również inne obowiązki wynikające z przepisów RODO.

Obowiązki informacyjne

Obowiązek informacyjny wobec osoby fizycznej, której dane są przetwarzane, w tym pracownika (art. 13 RODO), powinien nastąpić podczas pozyskiwania danych osobowych. W przypadku klientów biura księgowego powinien być utrwalony w umowie z klientem.

Z kolei w przypadku pozyskania danych z innego źródła (np.danych z CEIDG) obowiązek powinien zostać wykonany, najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych (art. 14 ust. 3 lit. a RODO).

Przykład

Przedsiębiorca odebrał zgody pracowników na przetwarzanie danych osobowych w celu wykonania specjalnych identyfikatorów wejściowych ze zdjęciem pracowników. W tym przypadku oprócz potrzeby uzyskania zgody z określeniem celu przetwarzania danych czyli dla wyrobienia identyfikatora, konieczne jest też przekazanie klauzuli informacyjnej o przetwarzaniu danych w celu wrobienia i inwentaryzacji identyfikatorów.

Art. 7 RODO

Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych

Obowiązek prowadzenie rejestru czynności przetwarzania danych

Każdy administrator i przetwarzający dane jest zobowiązany do prowadzenia wewnętrznego rejestru czynności przetwarzania danych.

RODO wskazuje wyłączenia (zwolnieni tylko ci przedsiębiorcy lub podmioty zatrudniające mniej niż 250 osób, przetwarzanie ma charakter sporadyczny i nie powoduje ryzyka naruszenia praw i wolności osób których dane dotyczą) ale to wyłączenie w znakomitej większości przypadków nie będzie dotyczyło biur księgowych, bo nie będzie miało choćby charakteru sporadycznego. Art. 30 RODO

Co powinien zawierać rejestr

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także inspektora ochrony danych – jeśli został ustanowiony,

- cele przetwarzania, np. w procesie rekrutacji pobieranie dokumentów aplikacyjnych, lub w procesie wypełniania deklaracji podatkowych pobieranie danych identyfikacyjnych

- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych – np.. klienci, pracownicy, kandydaci

- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych, - np. urząd skarbowy, ZUS

- informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej,

- jeżeli jest to możliwe – planowane terminy usunięcia poszczególnych kategorii danych,

- jeżeli jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Rejestry muszą mieć formę pisemną, przy czym mogą być sporządzone również w formie elektronicznej (art. 30 ust. 3 RODO).

Obowiązek przeprowadzenia analizy ryzyka

Zgodnie z art. 32 RODO uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Aby wdrożyć odpowiednie środki, należy przeprowadzić analizę ryzyka bezpieczeństwa danych osobowych.

Analiza ryzyka będzie to wynik porównania prawdopodobieństwa wystąpienia określonego zdarzenia negatywnego oraz ciężkości jego następstw dla osoby której dane dotyczą np. ryzyko utraty dokumentów źródłowych w postaci kradzieży i ujawnienia danych, lub ryzyko utraty dokumentów źródłowych wskutek zalania.

Dopiero po identyfikacji ryzyka pozwoli nam na wypełnienie obowiązków z art. 32 RODO i dostosowanie adekwatnych zabezpieczeń, czy fizycznych, czy organizacyjnych albo informatycznych.

Obowiązek wdrożenia procedur ochrony danych osobowych

Art. 24 ust. 1 RODO wskazuje na konieczność wdrożenia polityk ochrony danych przez administratora danych osobowych. Nie sprecyzowano natomiast, jakie to mają być polityki ani co muszą zawierać. Przepisy RODO pozostawiły w tym zakresie dowolność administratorom danych, w zależności od ich profilu biznesowego. Przydatne mogą okazać się dokumenty w postaci polityki ochrony danych osobowych, instrukcje zarządzania systemem informatycznym czy książka dobrych praktyk.

Obowiązek wyznaczenia insektora danych osobowych

Art. 37 RODO nakazuje wyznaczyć inspektora ochrony danych, m.in. gdy: główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.

Pytanie o znaczenie wyrażenia „dużej skali”

Zgłaszanie naruszeń ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – musi zgłaszać je organowi nadzorczemu czyli Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki musi ponadto zawiadamiać osobę, której danych to dotyczy, o takim naruszeniu.

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. Art. 33 RODO

Prowadzenie rejestru naruszeń

Rejestr naruszeń danych osobowych obejmuje zarówno te zdarzenia, które zostały zgłoszone organowi nadzorczemu, jak i zdarzenia, które nie zostały zgłoszone.

Przykład: biuro omyłkowo wysłało deklaracje na adres innego przedsiębiorcy niż właściwy adresat. W takim przypadku incydent ten powinien zostać odnotowany w rejestrze naruszeń. Jeśli deklaracja nie dotyczy danych o istotnym znaczeniu dla przedsiębiorcy, nie ma konieczności zgłaszania incydentu.

Programy księgowe

Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.