KANCELARIA PRAWA GOSPODARCZEGO
Kazimierz Wlazło
Aneta Guza-Wójtowicz

Radom, 13 kwietnia 2018r.

INFORMACJA DOT. RODO

RODO będzie stosowane **od 25 maja 2018 r.** Do tej daty **wszystkie te podmioty, które podlegają RODO, powinny być gotowe do stosowania RODO – nie będzie już żadnego dodatkowego okresu przejściowego.** RODO to 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). Jest to akt prawny przyjęty przez Unię Europejską regulujący zasady ochrony danych osobowych – zastępuje dyrektywę 95/46/WE z 1995 r.

RODO tym się różni od dyrektywy 95/46/WE, że nie będzie implementowane, czyli nie będzie trzeba przepisów RODO przyjąć w polskiej ustawie, jak to się dzieje w przypadku dyrektyw. **RODO będzie bezpośrednio obowiązywać, będzie bezpośrednio stosowane i bezpośrednio skuteczne.** To oznacza, że – z bardzo niewielkimi wyjątkami – całe prawo ochrony danych osobowych znajdziemy bezpośrednio w tekście RODO.

RODO zastąpi obowiązującą obecnie ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych, podlega mu każdy przedsiębiorca, który prowadzi działalność w Unii Europejskiej. Może to być działalność w jakiejkolwiek formie prawnej: spółka, jednoosobowa działalność gospodarcza, czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią. Nie ma znaczenia narodowość osób, których dane osobowe są przetwarzane. Nie ma znaczenia to, gdzie są przetwarzane dane osobowe (gdzie znajdują się serwery). RODO znajdzie zastosowanie nawet wtedy, gdy podmioty spoza Unii Europejskiej oferują swoje towary i usług osobom przebywający w Unii.

Obowiązkiem administratorów danych będzie **m.in. zgłaszanie w ciągu 72 godzin** od wykrycia do właściwego organu nadzoru przypadków naruszeń, które mogą skutkować zagrożeniem praw i swobód osób, których dane zostały naruszone. Może także wystąpić konieczność zawiadomienia konkretnej osoby, bez zbędnej zwłoki, o przypadku wystąpienia dużego ryzyka naruszenia jej praw lub swobód.

Przepisami RODO wprowadzone zostaje:

- „prawo do bycia zapomnianym” (skierowane do obywateli, którzy życzą sobie, by ich dane osobowe zostały usunięte),
- uprawnienie do żądania przeniesienia danych,

26-610 Radom
ul. Sienna 15

tel./fax (+48) 48 3778030
www.kancelariakpg.pl
kpg@kancelariakpg.pl

Kazimierz Wlazło i Aneta Guza-Wójtowicz
Spółka Partnerska Radców Prawnych
NIP 796 297 67 71
Bank ING BŚ S.A. Nr 23 1050 1793 1000 0092 3987 5918
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XIV Wydział Gospodarczy
KRS Nr: 0000669961

- oraz wzmocnione prawo dostępu i wglądu obywatela w jego dane.

Obowiązkiem niektórych firm zarówno kontrolujących, jak i przetwarzających dane, będzie **wyznaczenie Inspektora Ochrony Danych Osobowych**. Osoba ta musi dysponować wiedzą ekspercką w zakresie ochrony danych osobowych.

Kontrolujący i przetwarzający dane będą zobowiązani od **przygotowania i utrzymania wszechstronnych rejestrów** dotyczących przetwarzanych danych, uwzględniających m.in.: powody przetwarzania danych, kategorie podmiotów danych i danych osobowych, adresatów danych, rejestry międzynarodowych transferów danych, rejestry naruszeń i incydentów, rozwój i utrzymanie zasad ochrony prywatności dla każdej linii produktowej, przechowywanie potwierdzonych zgód na przetwarzanie danych itd.

Przepisami RODO zostają wprowadzone również **nowe lub uzupełnione zasady uzyskiwania ważnych i weryfikowalnych zgód na przetwarzanie danych osobowych od osób, których dane dotyczą.**

RODO stosuje się do przetwarzania danych osobowych. Przetwarzaniem danych osobowych są jakiekolwiek operacje wykonywane na danych osobowych, takie jak:
• zbieranie danych,
• przechowywanie danych,
• usuwanie danych,
• opracowywanie danych,
• udostępnianie danych.

Co bardzo ważne, RODO obejmuje wszelkie czynności, które mają za przedmiot dane osobowe – czyli nie tylko np. usługę archiwizowania dokumentów, ale wszelkie usługi, w których dochodzi do zbierania danych osobowych. RODO powinni więc stosować również **np. przedsiębiorcy, którzy przetwarzają dane osobowe przy okazji świadczenia innych usług**, np. pośrednicy ubezpieczeniowi, agenci biur podróży, księgowi, sklepy internetowe, zarządcy nieruchomości itp.

Przetwarzanie danych osobowych to **bardzo ogólne sformułowanie**, oznaczające jakiekolwiek operacje wykonywane na danych osobowych, takie jak:
• zbieranie danych,
• przechowywanie danych,
• usuwanie danych,
• opracowywanie danych,
• udostępnianie danych.

Jeżeli jakiś przedsiębiorca przetwarza dane osobowe, to może to robić jako jeden z dwóch kategorii podmiotów:

• administrator danych,

• podmiot przetwarzający dane.

Administrator danych to taki podmiot, który decyduje o celach i sposobach przetwarzania danych. Innymi słowy, decyduje o tym, po co (cele) i jak (sposoby) wykorzystać dane osobowe, np. pracodawca w stosunku do danych osobowych swoich pracowników, sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów.

Administratorem danych jest zawsze określony podmiot – np. spółka (nie jej pracownik) lub osoba fizyczna prowadząca działalność gospodarczą.

Podmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego, np. biuro rachunkowe przetwarza na zlecenie dane osobowe przekazane mu w tym celu przez klientów.

Podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych odpowiednią umowę, **tzw. umowę powierzenia**, w której określone zostaną zasady przetwarzania danych.

W danej organizacji, dane osobowe faktycznie przetwarzają konkretne osoby fizyczne – pracownicy lub współpracownicy administratora lub podmiotu przetwarzającego dane. Takie osoby powinny posiadać upoważnienie do przetwarzania danych osobowych.

Dane osobowe można przetwarzać wyłącznie wtedy, gdy istnieje tzw. podstawa prawna przetwarzania danych. W przypadku przedsiębiorców, typowymi podstawami przetwarzania danych zwykłych są:

a) zgoda osoby, której dane dotyczą,

b) przetwarzanie danych jest niezbędne do wykonania umowy z osobą, której dane dotyczą lub do podjęcia działań poprzedzających zawarcie umowy, na żądanie tej osoby,

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

d) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

W przypadku szczególnych kategorii danych, typowe podstawy przetwarzania danych to:

a) wyraźna zgoda osoby, której dane dotyczą,

b) przetwarzanie danych jest niezbędne do wykonania zadań związanych z zatrudnieniem, ubezpieczeniem społecznym pracowników,
c) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy,
d) przetwarzanie danych jest niezbędne w celu dochodzenia praw przed sądem.

Zawsze to administrator danych powinien móc wykazać, że dysponuje odpowiednią podstawą przetwarzania danych. Jest to prawny obowiązek administratora danych wynikający z tzw. zasady rozliczalności.

Zgoda może zostać wyrażona w dowolnej formie – ale zawsze w razie wątpliwości to administrator danych powinien wykazać, że zgoda została udzielona. Decyzja o tym, jaki konkretnie sposób zbierania – i archiwizowania – zgód zastosować powinna być podjęta świadomie przez administratora danych.

RODO nakazuje, aby przy gromadzeniu danych przekazywać osobie, której dane dotyczą, szereg informacji:

• o tożsamości administratora danych i o jego danych kontaktowych,
• jeżeli administrator danych powołał Inspektora Ochrony Danych (IOD) – o danych kontaktowych IOD,
• o celach i podstawie przetwarzania danych, a jeżeli przetwarzanie odbywa się na tej podstawie, że jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – o tych prawnie uzasadnionych interesach,
• o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją
• gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego,
• o okresie czasu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
• o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
• jeżeli przetwarzanie odbywa się na podstawie zgody – o prawie do cofnięcia zgody w dowolnym momencie,
• o prawie wniesienia skargi do organu nadzorczego,

• o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
• jeżeli dochodzi do tzw. zautomatyzowanego podejmowania decyzji lub profilowania – należy poinformować o tym fakcie oraz podać istotne informacje o zasadach automatycznego podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Co istotne, odbiorcy danych to także podmioty przetwarzające dane osobowe na zlecenie administratora danych, stąd konieczność poinformowania o tych podmiotach.

Te – bardzo rozbudowane – obowiązki informacyjne w przypadku zgody na przetwarzanie danych osobowych przybierają najczęściej postać tzw. klauzuli zgody na przetwarzanie danych.

Kary za naruszenia przepisów rozporządzenia RODO:

Artykuł rozporządzenia	**Kara**
Art. 25 Naruszenie zasad ochrony danych osobowych w fazie projektowania (privacy by design) oraz domyślna ochrona danych (privacy by default)	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 29 Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 30 Rejestrowanie czynności przetwarzania	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 31 Współpraca z organem nadzorczym	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa

Art. 32 Bezpieczeństwo przetwarzania	10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 5 Naruszenie zasad dotyczących przetwarzania danych osobowych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 7 Naruszenie warunków wyrażenia zgody na przetwarzanie danych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 15 Naruszenie wykonania prawa dostępu przysługującego osobie, której dane dotyczą	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa
Art. 16 Naruszenie wykonania prawa do sprostowania i usuwania danych	20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa