5

RODO – UNIJNE ROZPORZĄDZENIE WYZWANIEM DLA PRZEDSIĘBIORCÓW

5.1 WSTĘP

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) – RODO – to nowy akt prawny o ochronie danych osobowych.

Formalnie RODO utrzymuje dotychczasowe zasady ochrony danych osobowych obowiązujące na terenie Unii Europejskiej, w tym w Polsce na podstawie starej ustawy z 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze zm.). Zasady te zostały doprecyzowane, prawa osób fizycznych nazwane, natomiast wprowadzone kary pieniężne zwracają uwagę dotychczas niespotykaną wysokością [1].

RODO ma na celu budowę nowego i jednolitego na poziomie UE systemu ochrony danych osobowych, który opiera się na: **legalności**, **respektowaniu i przestrzeganiu praw jednostki** oraz **zapewnieniu bezpieczeństwa danych**.

Administrator chcąc sprostać przepisom unijnym powinien podjąć szereg działań. Budując sprawny system przetwarzania danych osobowych w organizacji administrator powinien:

- znać ogólne zasady przetwarzania danych osobowych,
- wykazać właściwą podstawę prawną ich przetwarzania,
- prowadzić analizę ryzyka dla procesów przetwarzania danych osobowych,
- spełniać obowiązek informacyjny,
- pobierać zgody na przetwarzanie danych tam gdzie jest to konieczne i niezbędne,
- respektować prawa osób fizycznych uwzględniając proces profilowania,
- analizować i zgłaszać do organu naruszenia ochrony danych,
- prowadzić wymaganą dokumentację,
- przeanalizować zasadność powołania inspektora ochrony danych,
- poznać podstawy transgranicznego przepływu danych.

Działania te umożliwią funkcjonowanie przedsiębiorstwa zgodnie z wymogami RODO.

5.2 ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Administrator danych zobowiązany jest do zapewnienia przetwarzania danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"); do zbierania danych w konkretnych, wyraźnych, prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu"); do zbierania tylko tych danych, które są niezbędne do realizacji celu, tzw. "minimalizacja danych"; do zapewnienia, aby dane osobowe były prawidłowe i w razie potrzeby uaktualniane. Administrator powinien podjąć wszelkie działania, aby dane osobowe były „prawidłowe" w świetle celów ich przetwarzania i przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przechowywane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, bądź do celów statystycznych z zastrzeżeniem, że zostały wdrożone odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania"). Ponadto dane powinny być przetwarzane przez administratora w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkowa utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność") [2].
Administrator nie tylko jest odpowiedzialny za przestrzeganie przepisów i wymogów RODO, ale jednocześnie musi być w stanie wykazać przestrzeganie tych wytycznych, czyli zapewnić tzw. „rozliczalność".

5.3 WŁAŚCIWA PODSTAWA ZBIERANIA DANYCH OSOBOWYCH ORAZ ADEKWATNE ICH WYKORZYSTANIE

Przetwarzanie danych osobowych jest zgodne z prawem tylko i wyłącznie w przypadkach gdy Administrator spełnia, co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- 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;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, podyktowanego prawem Unii lub państwa członkowskiego;

- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą , lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- 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.

Warto dodać, że ten warunek nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań [2].

5.4 OBOWIĄZEK INFORMACYJNY

Jednym z głównych zadań, jakie RODO nałożyło na administratora jest konieczność spełniania w określonych sytuacjach obowiązku informacyjnego względem osób fizycznych. Podmiot danych ma prawo uzyskać szereg informacji na temat przetwarzania swoich danych osobowych od administratora. RODO nakazuje spełnianie obowiązku informacyjnego w dwóch sytuacjach: gdy dane zbierane są bezpośrednio od osoby, której one dotyczą, oraz w przypadku gromadzenia danych ze źródeł pośrednich, tj. nie od osoby, której one dotyczą. Kiedy spełnić ów obowiązek? W przypadku kiedy dane zbierane są bezpośrednio od podmiotu danych – w momencie pozyskiwania tych danych. W przypadku pośredniego zbierania danych obowiązek informacyjny należy spełnić w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca [2]. Obowiązek informacyjny musi zostać zrealizowany zgodnie z art.13 oraz art. 14 RODO i jest uzależniony od źródła pozyskania danych oraz jego relacji z osobą, której dane dotyczą. W sytuacji, w której administrator rozszerza zakres danych o podmiocie danych lub zmienia cel przetwarzania danych osobowych zobligowany jest do ponownego spełnienia obowiązku informacyjnego względem osoby której dane dotyczą.

Udzielenie informacji na temat przetwarzania danych osobowych przez administratora w postaci obowiązku informacyjnego nie jest jednak konieczne, jeżeli osoba fizyczna dysponuje już tymi informacjami, jeżeli utrwalenie lub ujawnienie danych są wyraźnie przewidziane prawem, lub jeżeli poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

5.5 RESPEKTOWANIE PRAW OSÓB KTÓRYCH DANE DOTYCZĄ

Unijne rozporządzenie gwarantuje podmiotowi danych, szereg praw, które musi realizować administrator.

5.5.1 Prawo dostępu do danych

Osoba, której dane dotyczą ma możliwość uzyskania od administratora informacji, czy jej dane są przetwarzane i w jakim zakresie. Komunikacja pomiędzy administratorem a podmiotem danych musi być prowadzona w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie.

Jeśli zajdzie taka potrzeba, osobie której dane dotyczą dostarcza się kopię danych osobowych podlegających przetwarzaniu. Kopia ta powinna zostać wydana bezpłatnie za pierwszym razem, przy kolejnych prośbach może zostać nałożona na wnioskującego rozsądna opłata, wynikająca np. z kosztów administracyjnych.

5.5.2 Prawo do sprostowania danych

Podmiot danych ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

5.5.3 Prawo do usunięcia danych „prawo do bycia zapomnianym"

Osoba fizyczna **ma prawo żądania niezwłocznego usunięcia** dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z przesłanek: dane osobowe **nie są już niezbędne do celów, w których zostały zebrane**; osoba, której dane dotyczą, **cofnęła zgodę**; osoba, której dane dotyczą, wnosi sprzeciw; dane osobowe były przetwarzane niezgodnie z prawem; dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego; dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego (przetwarzanie danych dzieci).

Jeżeli administrator upubliczniła dane osobowe to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że **osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje**.

Istnieją również sytuacje, które sprawiają, że osoby, których dane dotyczą nie mogą skorzystać z prawa do usunięcia danych osobowych. Mowa tu o przypadkach, kiedy przetwarzanie jest niezbędne: w celu korzystania z prawa do wolności wypowiedzi i informacji; do wywiązania się z prawnego obowiązku wymagającego przetwarzania

na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; w celu profilaktyki zdrowotnej (np. medycyna pracy, czy zapewnienie opieki zdrowotnej); do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych; do ustalenia, dochodzenia lub obrony roszczeń.

5.5.4 Prawo do ograniczenia przetwarzania

Prawo to rozumiane jest jako **oznaczenie przechowywanych danych osobowych**, zarówno w postaci elektronicznej, jak i w postaci papierowej, **w celu ograniczenia ich przyszłego przetwarzania** (nakaz przechowywania przez administratora dotychczas zebranych danych oraz brak możliwości dokonywania na nich innych operacji niż przechowywanie).

Osoba, której dane dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach: osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający sprawdzić prawidłowość tych danych; przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; Spółka nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń; osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Spółki są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

5.5.5 Prawo do przenoszenia danych

Podmiot danych, ma prawo otrzymać w **ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego** dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi, jeżeli przetwarzanie odbywa się na podstawie zgody osoby lub na podstawie umowy, przetwarzanie odbywa się w sposób zautomatyzowany i jest to technicznie możliwe.

5.5.6 Prawo do sprzeciwu

Osoba fizyczna ma prawo **wnieść sprzeciw** wobec przetwarzania dotyczących jej danych osobowych, w tym profilowania. Spółce nie wolno już wtedy przetwarzać tych danych osobowych, chyba że wykaże ona istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania.
Wyjątek stanowi sytuacja, kiedy to przeprowadzenie profilowania jest wymagane w celu prawidłowego zawarcia bądź wykonania umowy – wtedy osoba, której dane dotyczą nie ma prawa do sprzeciwu wobec takiego przetwarzania.
Mimo bogatego wachlarza praw RODO wprowadza podstawy do pewnych ograniczeń. Rozporządzenie uwzględnia pewne ograniczenia dla praw osób, których dane dotyczą w szczególnych przypadkach, np.: konieczność zapewnienia bezpieczeństwa narodowego lub publicznego; zapobieganie przestępczości; konieczność zapewnienia niezależności sądów; kiedy prawa osób, których dane dotyczą, utrudniają wypełnienie celów gospodarczych lub finansowych państwa członkowskiego lub Unii Europejskiej.

5.6 PROFILOWANIE

Profilowanie to dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się [3]. Profilowanie i zautomatyzowanie podejmowania decyzji wykorzystuje się w coraz liczniejszych sektorach, zarówno prywatnych jak i publicznych. Może to stanowić przydatne narzędzie dla osób fizycznych i organizacji, przynosząc takie korzyści jak: większa wydajność oraz oszczędność czasu. Jednak profilowanie i zautomatyzowane podejmowanie decyzji mogą stwarzać znaczne zagrożenia dla praw o wolności osób fizycznych, przez co konieczne jest zapewnienie odpowiednich zabezpieczeń.
Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i **wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.**
Nie ma to jednak zastosowania, jeżeli ta decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą bądź opiera się na wyraźnej zgodzie osoby, której dane dotyczą. Jeżeli administrator wykorzystuje profilowanie jest zobligowany do wdrożenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej **prawa do uzyskania interwencji ludzkiej** ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

5.7 ZGODA – W KAŻDEJ CHWILI MOŻE ZOSTAĆ WYCOFANA

Jedną z najczęściej stosowanych podstaw prawnych przetwarzania danych osobowych jest zgoda osoby fizycznej. Zgodnie z RODO zgoda oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych [2] w formie ustnej, pisemnej lub elektronicznej. Administrator musi pamiętać o tym, ze zgoda w każdej chwili może zostać przez podmiot danych odwołana, ale wycofanie tej zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Istotnym jest aby osoba, której dane dotyczą była o profilowaniu poinformowana zanim wyrazi zgodę na przetwarzanie swoich danych osobowych. Dodatkowo wycofanie zgody powinno być równie łatwe jak jej wyrażenie, co powoduje konieczność zastosowania odpowiednich rozwiązań technicznych.

Kwestią uregulowaną przez RODO jest również przetwarzanie danych osobowych dzieci w ramach świadczenia usług społeczeństwa informacyjnego, np. korzystanie z portali społecznościowych, czy kont e-mail. Zgodnie z RODO w przypadku kiedy dochodzi do przetwarzania danych osobowych dziecka poniżej 16 roku życia, przetwarzanie takie jest zgodne z prawem, w sytuacji kiedy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła lub zaaprobowała zgodę. RODO pozwala państwom członkowskim na pewna swobodę i zastosowanie niższej granicy wiekowej, która musi wynosić, co najmniej 13 lat. Polski ustawodawca nie skorzystał z tej możliwości.

5.8 NARUSZENIA – PROCEDURA ZGŁASZANIA ORAZ INFORMOWANIE OSOBY, KTÓREJ DANE ZOSTAŁY NARUSZONE

W ogólnym rozporządzeniu o ochronie danych osobowych wprowadzono wymóg zgłaszania naruszeń ochrony danych osobowych właściwemu krajowemu organowi nadzorczemu lub w przypadku naruszeń o charakterze transgranicznym – wiodącemu organowi nadzorczemu, a w określonych przypadkach przekazywania informacji o naruszeniach osobom fizycznym, na których dane osobowe wywarły one wpływ [4].

Czym jest naruszenie ochrony danych osobowych? To naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych [2].

Co to oznacza dla administratora danych? W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi nadzorczemu. Administrator zobowiązany jest udokumentować naruszenie w rejestrze naruszeń, zgłosić je do

organu nadzorczego jakim jest Prezes Urzędu Ochrony Danych Osobowych i jeżeli zaistnieje taka konieczność powiadomić podmiot danych o naruszeniu jego danych osobowych. Wymóg zgłaszania naruszeń powoduje, że administrator zobligowany jest do opracowania stosownych planów z wyprzedzeniem i wdrażania procedur umożliwiających wykrywanie naruszeń i szybkie ograniczenie ich negatywnych skutków, ocenie ryzyka dla osób fizycznych, a następnie podejmowanie decyzji w kwestii tego, czy w danym przypadku zachodzi konieczność zgłaszania naruszenia organowi nadzorczemu, jak również zawiadomienia zainteresowanych osób fizycznych o naruszeniu.

5.9 DOKUMENTY – TYLKO NIEZBĘDNE MINIMUM

Administrator jest zobligowany do wykazania przestrzegania przepisów ogólnego rozporządzenia ochrony danych osobowych. Właściwym sposobem na realizację tego nakazu jest przyjęcie i stosowanie wewnętrznych polityk, regulaminów i instrukcji. Uwzględniając charakter, zakres, kontekst, cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator powinien wdrożyć odpowiednie środki organizacyjne i techniczne aby przetwarzanie odbywało się zgodnie z RODO. Środki o których mowa obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych [2].

Administrator powinien prowadzić rejestr czynności przetwarzania danych osobowych, za które odpowiada. Każdy podmiot przetwarzający, czyli ten, któremu powierzono dane powinien prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. Rejestry mają formę pisemną lub elektroniczną i są udostępniane na żądanie organu nadzorczego jakim jest Prezes Urzędu Ochrony Danych Osobowych.

Administrator zobligowany jest dokumentować wszelkie naruszenia ochrony danych osobowych w tym okoliczności naruszenia ochrony danych osobowych jego skutki oraz podjęte działania zaradcze.

Nadrzędnym dokumentem administratora jest polityka ochrony danych osobowych, w której zawarte mogą być m. in. cel i zakres polityki, zadania i odpowiedzialność odpowiedzialności osób funkcyjnych, pracowników oraz komórek organizacyjnych, gromadzenie oraz przepływ danych osobowych. Administrator ma zapewnić, że przyjęte w organizacji dokumenty odzwierciedlają zasady przetwarzania danych osobowych i są stosowane zgodnie z RODO.

Warto aby polityki były wzbogacone o procedury i instrukcje regulujące, np. proces realizacji praw osób, których dane dotyczą, zarządzanie zgodami i spełnieniem obowiązku informacyjnego, sposób zarzadzania naruszeniami, proces nadawania upoważnień do przetwarzania danych osobowych, proces analizy ryzyka, procedury regulujące zabezpieczenia fizyczne, techniczne i teleinformatyczne.

5.10 INSPEKTOR OCHRONY DANYCH

Obowiązkiem niektórych administratorów i podmiotów przetwarzających jest powołanie inspektora ochrony danych (IOD). Wyznaczenie IOD jest obowiązkowe gdy przetwarzania dokonują organ lub podmiot publiczny (niezależnie od tego, jakie dane są przetwarzane); główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnej kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Administrator, który nie jest zobowiązany przepisami prawa do wyznaczenia IOD i nie zamierza dobrowolnie wyznaczyć takiego inspektora, może wyznaczyć pracownika, albo zatrudnić zewnętrznego konsultanta do wypełniania zadań związanych z ochroną danych osobowych. W przypadku powołania takiej osoby istotne jest, aby nazwa stanowiska, status pracownika, pozycja i zadania nie wprowadzały w błąd. Administrator powinien poinformować pracowników organizacji, organ ochrony danych osobowych, osoby, których dane dotyczą i ogół społeczeństwa, że osoba zatrudniona nie jest IOD w świetle przepisów RODO.

Artykuł 37 RODO stanowi, że grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile „można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej" [2].

W celu zapewnienia możliwości łatwego kontaktu z IOD, czy to wewnętrznym, czy zewnętrznym, istotne jest udostepnienie jego danych kontaktowych. Komunikacja musi odbywać się w językach używanych przez organy nadzorcze i osoby, których dane dotyczą. Dostępność IOD ma znaczenie dla zapewnienia, że podmiot danych może bez problemy skontaktować się z IOD [5].

Istotne jest by Inspektor Ochrony Danych posiadał odpowiednia wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość RODO. Przydatna jest również wiedza danego sektora podmiotu danych.[5] Wykonując swoje zadania ważne jest aby DPO był zaangażowany we wszystkie kwestie związane z ochroną danych w tym nowe projekty. Miał do dyspozycji odpowiednie zasoby, mógł wykonywać swoje zadania w sposób niezależny. Warto przypomnieć, że inspektor ochrony danych podlega bezpośrednio pod najwyższe kierownictwo.

5.11 PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH – ODPOWIEDNI STOPIEŃ OCHRONY DANYCH OSOBOWYCH

Przekazywanie danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w RODO, gdy Komisja stwierdzi, że państwo trzecie, terytorium, określony sektor lub określone

sektory w tym państwie trzecim bądź dana organizacja międzynarodowa, zapewniają odpowiedni stopień ochrony. W takich przypadkach, przekazywanie danych osobowych, może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Po dokonaniu oceny czy stopień ochrony jest odpowiedni, Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że dany podmiot zapewnia odpowiedni stopień ochrony [2].

W razie braku decyzji stwierdzającej odpowiedni stopień ochrony, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie gdy zapewnią odpowiednie zabezpieczenia i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej [2].

Należy zwrócić uwagę że zezwolenia wydane przez państwo członkowskie lub organ nadzorczy na mocy dotychczasowej dyrektywy (95/46/WE) jak i decyzje przyjęte przez Komisję na mocy powyższego dokumentu, zachowują ważność do czasu ich zmiany, zastąpienia lub uchylenia przez ten organ lub Komisję.

W razie braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń, przekazanie danych osobowych do państwa trzeciego jest możliwe pod warunkiem, że:

- osoba, której dane dotyczą, zostanie poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie oraz wyraźnie wyrazi na nie zgodę;
- przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą;
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą, między administratorem a inną osobą fizyczną lub prawną;
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;
- przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń;
- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes, ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego [2].

Przekazanie danych osobowych do państwa trzeciego może nastąpić wyłącznie, gdy nie jest ono powtarzalne; dotyczy tylko ograniczonej liczby osób, których dane dotyczą; jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą; administrator ocenił

wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych [2].
Ponadto administrator ma obowiązek poinformować organ nadzorczy oraz osobę, którą dane dotyczą o przekazaniu danych osobowych poza Europejski Obszar Gospodarczy. Administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie zabezpieczenia w rejestrach czynności przetwarzania.

5.12 PODSUMOWANIE

Ogólne rozporządzenie o ochronie danych osobowych jest aktem, który z jednej strony unifikuje obszar ochrony danych w państwach członkowskich Unii Europejskiej, a z drugiej strony może uchodzić za nieprecyzyjne. Warto jednak patrzeć na ten temat jako na szansę. Zamiarem unijnego regulatora było wprowadzenie aktu elastycznego, który proponuje podejście w oparciu o analizę ryzyka. Odpowiedzialność i adekwatność w każdej organizacji są rozpoznawane właśnie w wyniku analizy i wówczas administrator precyzuje zasady bezpieczeństwa przetwarzania danych osobowych. Analizując ryzyko utraty, uszkodzenia, czy wycieku danych osobowych lub nieadekwatnego przetwarzania w odniesieniu do działalności, administrator naraża się na zarzut ze strony organu nadzorczego jakim jest Prezes Urzędu Ochrony Danych nienależytej ochrony, nieadekwatnych zabezpieczeń zastosowanych do ochrony przetwarzanych przez siebie danych osobowych. Co w konsekwencji może doprowadzić do nałożenia na administratora wysokich kar pieniężnych wynikających z RODO, a w skrajnych przypadkach kary grzywny i pozbawienia wolności do lat 3, zgodnie z art. 107 i art. 108 nowej ustawy o ochronie danych osobowych.

LITERATURA

1. Gawroński M. red.: *RODO przewodnik ze wzorami*. Wolters Kluwer. Warszawa, 2018.
2. Sibiga G., Syska K.: *Ogólne rozporządzenie o ochronie danych. Podręczny zbiór przepisów o ochronie danych osobowych, zestawień, schematów, oraz wzorów rejestru czynności przetwarzania*. Wydawnictwo C.H. Beck, Warszawa 2017.
3. Grupa Robocza Artykułu 29: Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia WP-251, wersja po zmianach z dnia 6 lutego 2018r.
4. Grupa Robocza Artykułu 29: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem WP-250, wersja po zmianach z dnia 6 lutego 2018r.
5. Grupa Robocza Artykułu 29: Wytyczne dotyczące inspektorów ochrony danych WP-243, wersja po zmianach z dnia 5 kwietnia 2018r.

Data przesłania artykułu do Redakcji: 12.2018
Data akceptacji artykułu przez Redakcję: 02.2019

RODO – UNIJNE ROZPORZĄDZENIE WYZWANIEM DLA PRZEDSIĘBIORCÓW

Streszczenie: W artykule przedstawiono najważniejsze zadania administratora, które powinny być realizowane aby sprostać wymaganiom RODO. Przedstawiono także wskazówki jakie należy uwzględnić w wdrażaniu wytycznych unijnego rozporządzenia. Zwrócono uwagę na problem transgranicznego przekazywania danych do państw trzecich i wyzwania jakie stoją przed administratorem w tym zakresie.

Słowa kluczowe: administrator, inspektor ochrony danych, obowiązek informacyjny, zgoda, podmiot danych (osoba fizyczna), profilowanie, naruszenia ochrony danych, państwo trzecie, Prezes Urzędu Ochrony Danych Osobowych

GENERAL DATA PROTECTION REGULATION – EU REGULATION AS A CHALLENGE FOR ENTREPRENEURS

Abstract: The article presents Controller's most important tasks, which have to be fulfilled to meet the requirements of General Data Protection Regulation. Described guidelines are recommended in the process of implementing the EU regulation. Attention is paid to the problem of cross-border data transfer to third countries and the challenges that the Controller faces in this regard.

Key words: controller, data protection officer, information obligations, consent, data subject, profiling, data breach, third country, President of the Personal Character Data Protection

mgr Marzena Smolarska
FAMUR S.A.
ul. Armii Krajowej 51, 40-698 Katowice, Polska
tel. +48 781 550 418
e-mail: msmolarska@famur.com