STYCZEŃ 2019 / NR 1

OCHRONA DANYCH OSOBOWYCH

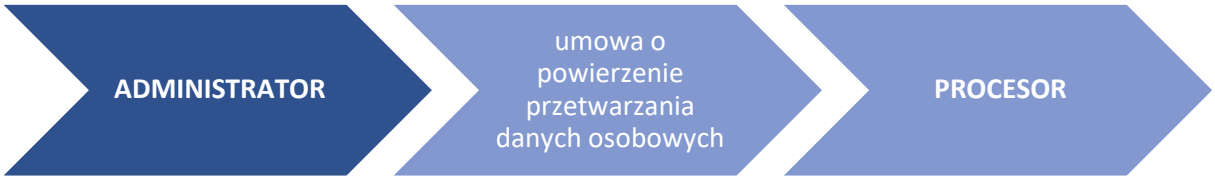
Miesięczny Newsletter

Kancelaria Wojciechowska Wojciechowski Radcowie Prawni Spółka Partnerska

W STYCZNIOWYM NUMERZE:

CZY NA PEWNO MASZ UMOWĘ PRZETWARZANIA DANYCH OSOBOWYCH?

Coraz częściej słyszy się o **kontrolach zgodności przetwarzania danych osobowych z RODO** przeprowadzanych przez państwa członkowskie Unii Europejskiej. O ile jednak do tej pory duży nacisk kładziono przede wszystkim na wypełnianie obowiązku informacyjnego czy też prawidłowe zbieranie zgód na przetwarzanie danych osobowych, o tyle obecnie wzmożone zostały **kontrole** związane z posiadaniem przez administratorów danych osobowych odpowiednich **umów o powierzenie przetwarzania danych** z Procesorem.



Najwięcej kontroli w tym zakresie przeprowadził duński organ nadzorczy, jednakże to w Niemczech nałożono pierwszą **karę finansową za brak umowy** o powierzenie przetwarzania danych osobowych w wysokości **5.000 EUR.** Kontrola była wynikiem skargi złożonej na małą firmę wysyłkową w Hesji, jednym z krajów związkowych Niemiec.

Przepisy RODO w kwestii przekazywania danych osobowych posługują się dwiema kategoriami podmiotów otrzymujących te dane - są to:

odbiorca i podmiot przetwarzający (tzw. procesor)

W dużym uproszczeniu, podmiot przetwarzający można zdefiniować jako **podmiot, który przetwarza dane osobowe w imieniu i na zlecenie administratora danych osobowych.** Jego cechą charakterystyczną jest zatem to, że w zakresie przetwarzania danych osobowych jest niejako uzależniony od administratora, wykonując tylko wskazane przez niego operacje na danych (procesor nie decyduje samodzielnie o celach i sposobach przetwarzania danych i zobowiązany jest np. zaprzestać przetwarzania danych gdy administrator zrezygnuje z jego usług). Odbiorcą jest zaś podmiot, któremu administrator przekazuje dane osobowe, ale podmiot ten dysponuje własnymi podstawami ich przetwarzania, samodzielnie ustala cele i sposoby tego przetwarzania, przez co staje się samoistnym administratorem danych.

Typowym przykładem **odbiorcy** jest **bank**, na którego przepisy prawa nakładają osobne obowiązki związane z przetwarzaniem danych osobowych (np. związane z przeciwdziałaniem praniu brudnych pieniędzy), a za **procesora** uważa się np. **biuro księgowe** świadczące zewnętrzne usługi księgowe na rzecz przedsiębiorcy.

Umowa o powierzenie przetwarzania danych osobowych

Zgodnie z art. 28 ust. 1 RODO administrator powinien korzystać wyłącznie z usług podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych służących bezpieczeństwu danych osobowych. Na gruncie RODO **Administrator i Procesor działają wspólnie** w celu spełnienia obowiązków wynikających z Rozporządzenia, co oznacza, iż Procesor zobowiązany jest do aktywnego pomagania Administratorowi w wypełnianiu ww. obowiązków. Warto też wspomnieć, iż aktualnie trwają konsultacje społeczne w sprawie opracowania przez PUODO standardowych klauzul umownych, o których mowa w art. 28 ust. 8 RODO.

Umowa powierzenia przetwarzania danych osobowych

- przedmiot przetwarzania,
- czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych,
- kategorię osób, których dane dotyczą,
- obowiązki i prawa administratora,
- obowiązki podmiotu przetwarzającego.

AKTA PRACOWNICZE ZGODNE Z RODO

Z dniem **1 stycznia 2019 roku** weszły w życie duże zmiany w zakresie przechowywania dokumentacji pracowniczej. Nowe **Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej** dzieli dokumentację na akta osobowe oraz dokumentację w sprawach związanych ze stosunkiem pracy. Nowe zasady przechowywania dokumentacji pracowniczej dotyczą wszelkich dokumentów pracowniczych zgromadzonych po 1 stycznia 2019 roku, natomiast dokumentacja zgromadzona przed tą datą może pozostać bez zmian.

- **Część A** – wszelka dokumentacja zgromadzona w związku z procesem rekrutacji, tj. przed podjęciem zatrudnienia
- **Część B** – dokumenty związane z zatrudnieniem, tj. umowa o pracę, upoważnienie do przetwarzania danych osobowych, itp.
- **Część C** – dokumentacja związana z rozwiązaniem lub wygaśnięciem stosunku pracy, np. wypowiedzenie umowy o pracę
- **Część D** – dokumentacja związana z ponoszeniem przez pracownika odpowiedzialności porządkowej lub dyscyplinarnej

Nowe akta osobowe można usunąć **po 10 latach**, natomiast pozostałe **po 50 latach**, chyba że spełni się wymogi określone w ustawie o systemie ubezpieczeń społecznych.

Kara dla Google!

Francuski urząd nadzoru ochrony danych osobowych nałożył na firmę Google aż **57 milionów dolarów kary finansowej** za naruszenie RODO. Kontrola została wszczęta z uwagi na wniesione przez podmioty **skargi dotyczące naruszenia obowiązków informacyjnych**. Google nie tylko w sposób nienależyty informował o wykorzystywaniu danych osobowych swoich użytkowników, lecz również narzucał akceptację regulaminu, zaś dotarcie do informacji dotyczących przetwarzania danych osobowych było utrudnione (wskazano, iż wymagano aż 5-6 kliknięć, aby odnaleźć stosowne informacje). **To pierwsza tak duża kara** nałożona na firmę na gruncie RODO, ale z pewnością nie ostatnia.

Kolejny wyciek danych!

Jak podaje Niebezpiecznik.pl jeden z jego czytelników przypadkiem trafił na pliki zawierające dane osobowe klientów Freshmail. Serwis został natychmiastowo poinformowany o lukach w zabezpieczeniach, a **wyciek został zgłoszony do PUODO**. Jak wskazuje portal podmioty, których dane dotyczą nie zostali poinformowani o naruszeniu, gdyż firma uznała, iż **nie zachodzi obawa zagrożenia praw i wolności tych osób**. Freshmail niezwłocznie podjął kroki w celu zabezpieczenia ujawnionych plików, a odkrywca wycieku, który zgłosił sprawę do firmy został nagrodzony w ramach tzw. **bug bounty.** To kolejny głośny przypadek wycieku danych osobowych, zaraz po incydencie z Morele.net.

Pół roku stosowania RODO

Podsumowując pół roku stosowania RODO Prezes UODO podkreśliła, iż dzięki Rozporządzeniu wiele firm wdrożyło rozwiązania mające na celu nie tylko ochronę danych osobowych, lecz również **budowanie zaufania** do swoich klientów. A ci są **coraz bardziej świadomi** przysługujących im praw – w ciągu pół roku stosowania RODO zgłoszono do urzędu ponad **3 tysiące skarg**. Trzeba przy tym pamiętać, że to właśnie skargi klientów są najczęstszą przyczyną kontroli, które mogą skutkować nałożeniem na firmy **kar finansowych**. Liczba ta jednak, w porównaniu do innych państw Unii Europejskiej nie jest wygórowana – w Holandii liczba skarg za cały 2018 r. wyniosła prawie 21 tysięcy, z czego 29% skarg dotyczyło sektora medycznego, 26% administracji publicznej, a 17% usług finansowych. Warto zwrócić uwagę, że skargi te najczęściej dotyczyły przesłania danych osobowych do złego odbiorcy (63% skarg). Pozostałe skargi dotyczyły głównie utraty danych osobowych poprzez kradzież urządzeń (laptopów, nośników danych) oraz w wyniku ataków hakerskich, phishingu lub malware.

Kolejne skargi na zagranicznych gigantów!

Amazon, Spotify, Youtube, Apple, Netflix, Soundclous, Dazn to kolejne serwery, których działania pod kątem ochrony danych osobowych wzbudziły wśród użytkowników wiele wątpliwości. Noyb, czyli inicjator akcji, informuje, iż na chwilę obecną złożył już **10 skarg** w stosunku do wyżej wymienionych spółek. Skargi dotyczą przede wszystkim braku reakcji na żądania użytkowników lub trudności w ich realizacji oraz brak transparentności co do przetwarzanych danych osobowych, wiążący się z nienależytym spełnianiem obowiązków informacyjnych.

ZUS prosi o dane osobowe!

W ostatnim czasie przedsiębiorcy często otrzymywali e-maile z Zakładu Ubezpieczeń Społecznych, w których to urząd prosił ich o informacje dotyczące kontroli prawidłowości wykorzystywania zaświadczeń lekarskich przez pracowników. W wiadomościach tych ZUS prosił o podanie **szerokiego zakresu danych osobowych**, które miały zostać wpisane do przygotowanego przez urząd formularza Excel i po uzupełnieniu odesłane na adres e-mail właściwego oddziału ZUS. Pracodawców oburzył nie tylko fakt, iż muszą dokonywać kontroli za urząd, lecz również niskie standardy ZUSu w zakresie ochrony danych osobowych (brak szyfrowania wiadomości z danymi).

IAB i Google pod ostrzałem

Tym razem to Fundacja Panoptykon jest autorem skargi złożonej na Google oraz IAB (Interactive Advertising Bureau) w związku z przetwarzaniem danych osobowych użytkowników w procesie prowadzenia aukcji reklam emitowanych w internecie. Według Fundacji **dane wykorzystywane są w sposób niekontrolowany**, zapewniając do nich dostęp na szeroką skalę przy jednoczesnym braku mechanizmów pozwalających na nadzór nad tym, jak i przez kogo są one wykorzystywane.

Kontrole UODO

Prezes UODO zatwierdził **plan kontroli** na najbliższe miesiące. Wynika z niego, że w ramach sektora prywatnego kontroli spodziewać mogą się przedsiębiorcy z branży telemarketingowej, brokerzy danych, sektor bankowy i ubezpieczeniowy w kontekście profilowania oraz pracodawcy pod kątem stosowania monitoringu wizyjnego i przetwarzania danych w związku z rekrutacją.

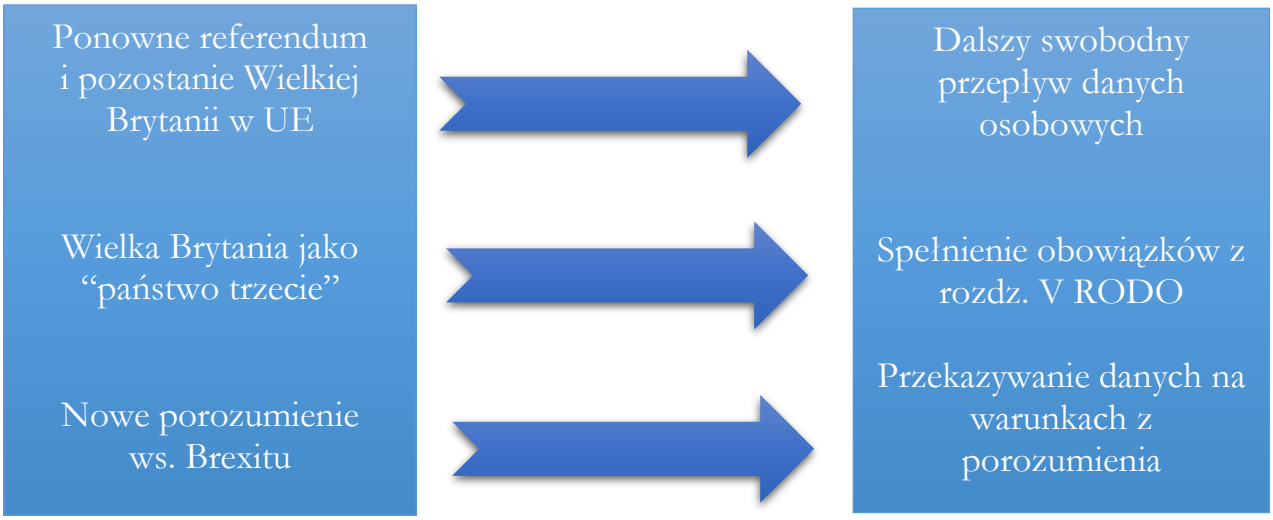
Wytyczne Ministerstwa Cyfryzacji dot. stosowania RODO

Minister Cyfryzacji opublikował **objaśnienia dotyczące przetwarzania danych osobowych osób ubiegających się o zatrudnienie u pracodawcy po zakończeniu rekrutacji**. Celem objaśnień jest wyjaśnienie wątpliwości w zakresie możliwości gromadzenia przez pracodawców dokumentów rekrutacyjnych już po zakończeniu procesu rekrutacji w stosunku do osób, które nie zostały zatrudnione. Wytyczne Ministerstwa stanowią zbiór **nieoficjalnych wskazówek** dla przedsiębiorców, jednakże należy pamiętać, iż ostatecznie to Prezes Urzędu Ochrony Danych Osobowych ma status i kompetencje organu nadzorczego określone w RODO.

BREXIT A OCHRONA DANYCH OSOBOWYCH

15 stycznia 2019 roku **Izba Gmin odrzuciła projekt porozumienia między Londynem a Brukselą** dotyczącego wyjścia Wielkiej Brytanii z Unii Europejskiej (UE). Projekt ten regulował wiele istotnych z punktu widzenia przedsiębiorców prowadzących interesy w Wielkiej Brytanii spraw, wśród nich oczywiście kwestie związane z ochroną danych osobowych. Wydaje się, że **Brexit jest już w sumie przesądzony**, a jedyną niewiadomą pozostają jego warunki.

Istnieją trzy możliwe rozwiązania:



Zgodnie z **informacją udostępnioną przez Prezesa UODO**, każdy administrator danych lub podmiot przetwarzający, którzy obecnie przekazują dane do Wielkiej Brytanii, powinien:

1. Zidentyfikować, jakie dane, w jakich celach i na jakiej podstawie prawnej są obecnie przekazywane do Wielkiej Brytanii;
2. Zdecydować, czy te transfery będą kontynuowane **po 29 marca 2019 r.;**
3. Wybrać i **wdrożyć odpowiedni mechanizm**, bądź podstawę prawną umożliwiającą przekazywanie danych;
4. W razie potrzeby zmodyfikować:
   a) wewnętrzną dokumentację przetwarzania danych, w tym rejestr czynności przetwarzania,
   b) klauzule informacyjne,
   c) istniejące wiążące reguły korporacyjne;
5. **Śledzić informacje dotyczące przebiegu procesu wyjścia Wielkiej Brytanii z UE**, gdyż nie jest jeszcze pewne na jakich zasadach to nastąpi, co może mieć wpływ na obowiązki związane z transferem danych.

W związku z tym niezbędne jest **przeanalizowanie danych osobowych** przekazywanych do Wielkiej Brytanii oraz **wszelkich związanych z tym aspektów** (podstaw przetwarzania, celu, itd.). Najdogodniejszym rozwiązaniem zapewniającym zgodność przekazywania danych osobowych do państw trzecich jest stosowanie standardowych klauzul umownych ochrony danych, zgodnie z Decyzjami Komisji Europejskiej (decyzja 2001/497/WE, decyzja 2004/915/WE, decyzja 2010/87/UE).

Art. 49 RODO wprowadza jednak **szereg wyjątków**, które zastosowanie znajdą w szczególnych przypadkach, gdy brak jest odpowiednich zabezpieczeń związanych z ochroną danych osobowych. Możliwe jest więc przekazanie danych osobowych do państwa trzeciego w przypadku, gdy:

- Administrator uzyskał **wyraźną zgodę** osoby, której dane mają zostać przekazane i poinformował ją o ryzyku z tym związanym;
- przekazanie jest **niezbędne do wykonania umowy** lub podjęcia środków przedumownych 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**, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- 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.

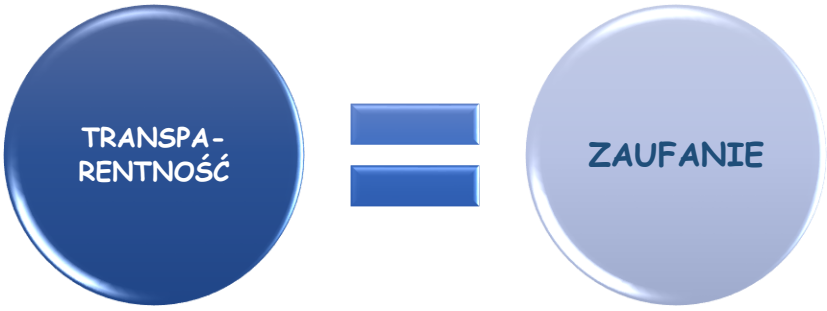
Oczywiście najlepszym z punktu widzenia przedsiębiorców rozwiązaniem byłoby uznanie przez Komisję Europejską, że Wielka Brytania jest państwem, które zapewnia odpowiedni stopień ochrony danych osobowych (art. 45 RODO). Jednakże proces wydawania takiej decyzji trwa miesiącami lub nawet latami. Jeśli dojdzie do **tzw. twardego Brexitu**, to Wielka Brytania przestanie być członkiem Unii Europejskiej już od 29 marca 2019 roku, co oznacza, że Komisja Europejska nie zdąży z wydaniem stosownej decyzji. W związku tym pozostaje mieć nadzieję, iż strony opracują dogodne porozumienie w zakresie przekazywania danych osobowych do Wielkiej Brytanii.

W JAKIM KIERUNKU ZMIERZA USTAWA WDRAŻAJĄCA RODO?

	ZAKRES ZMIAN
PRACODAWCA	wykształcenie i przebieg zatrudnienia kandydata do pracy możliwe do poznania jedynie, gdy jest to niezbędne ze względu na wykonywane stanowisko
	adres zamieszkania jedynie po zatrudnieniu kandydata do pracy - na etapie rekrutacji kandydat będzie mógł podać wybraną przez siebie formę kontaktu i ograniczyć ją np. tylko do numeru telefonu
	zakaz zbierania danych o niekaralności
	gromadzenie szczególnych kategorii danych jedynie za zgodą pracownika i z jego inicjatywy
ZWIĄZKI ZAWODOWE	bezwzględny zakaz monitorowania pomieszczeń udostępnianych zakładowej organizacji związkowej
ZFŚS	coroczny przegląd danych osobowych
	regulacja formy udostępnienia danych osób uprawnionych do świadczeń oraz okresu ich przechowywania

PRAWO DO INFORMACJI – CO MUSISZ WIEDZIEĆ?

Zgodnie z raportem firmy doradczej Deloitte podstawą zaufania konsumentów jest etyczne wykorzystywanie przez firmy informacji na ich temat. Przyznaje to aż **69 proc. respondentów**. Dlatego tak istotne jest rzetelne wypełnianie obowiązków informacyjnych spoczywających na Administratorze. **Świadomość klientów** w związku z wejściem w życie RODO nieustannie wzrasta i coraz chętniej korzystają oni z przysługujących im praw. Warto pamiętać, że im więcej informacji udzielimy klientom, tym mniejsze prawdopodobieństwo, że wystąpią ze skargą do organu nadzoru.



Podmioty, których dane dotyczą powinny być w sposób rzetelny informowane o tym, kto i w jakim celu przetwarza ich dane osobowe, jak długo przetwarzanie będzie trwało, jaka jest jego podstawa

prawna, jak można skontaktować się z Administratorem oraz jakie prawa przysługują podmiotom i w jaki sposób je realizować.

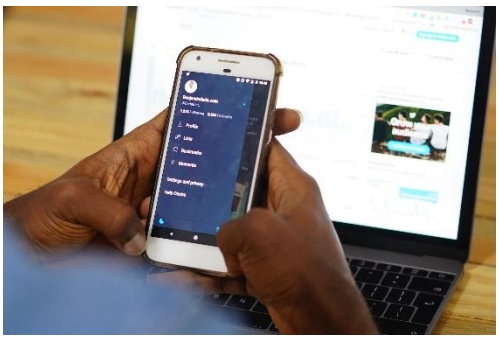
Trzeba też pamiętać, że **prawo do informacji sięga znacznie dalej**. Jak pokazują przeprowadzone przez organy nadzoru kontrole, przekazywane przez Administratora informacje muszą być przekazane:

- **w sposób prosty i zrozumiały** – to znaczy, że Administrator powinien dołożyć starań, aby informacje zawarte np. w klauzulach informacyjnych nie były zawiłe czy napisane trudnym do zrozumienia językiem,
- **w sposób transparentny** – oznacza to, że Administrator powinien rzetelnie przekazać wszystkie wymagane przez Rozporządzenie informacje,
- **w sposób łatwo dostępny** – informacje nie mogą być ukryte na stronie internetowej lub wymagać od podmiotów podejmowania skomplikowanych działań, dostęp do informacji powinien być szybki i prosty.

Administrator oprócz informowania o przetwarzaniu danych osobowych z własnej inicjatywy powinien również wdrożyć **odpowiednie środki** celem umożliwienia podmiotom realizacji ich praw związanych z uzyskaniem informacji na temat ich danych, np. poprzez udzielanie odpowiedzi na pytania i żądania podmiotów.

Przykładowe pytania, jakie można uzyskać:

- czy przetwarzają Państwo moje dane osobowe?
- Skąd mają Państwo mój adres?
- Jakie dane Państwo przetwarzają?
- Po co Państwu mój adres e-mail?
- Czy mogę uzyskać kopię moich danych, które Państwo przetwarzają?



Na każde pytanie skierowane przez podmiot należy udzielić wyczerpującej odpowiedzi **w terminie miesiąca od dnia uzyskania zapytania.** Brak reakcji ze strony Administratora lub lakonicznie udzielona odpowiedź może skutkować skargą do organu nadzorczego oraz utrata zaufania klientów i kontrahentów.

Prawo do informacji jest więc jedynym z najważniejszych praw, które przysługują podmiotom, co oznacza, że należy w sposób **przemyślany i rzetelny** wdrożyć instrumenty, które pozwolą na jego realizację.