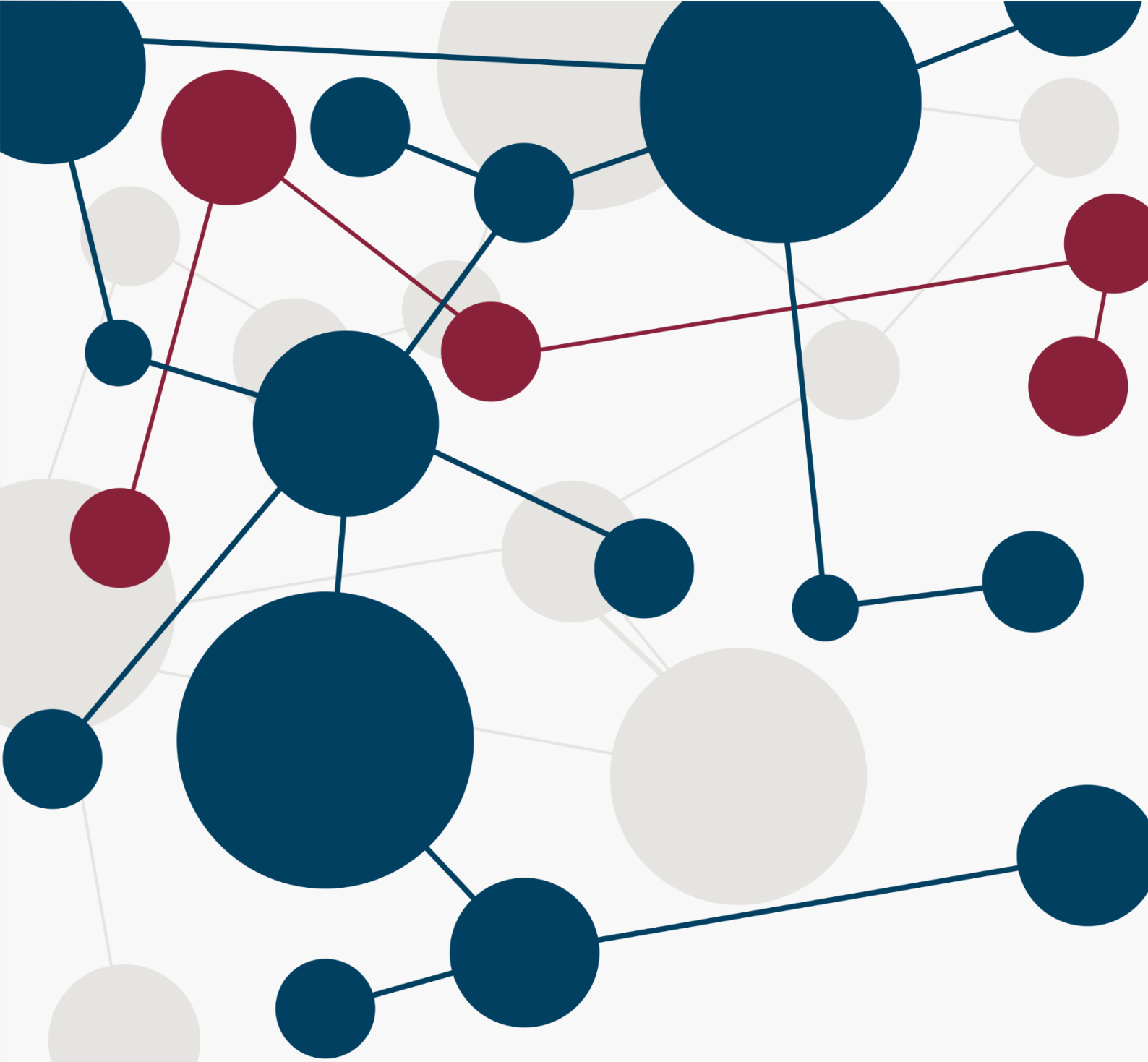


RODO 2018

wprowadzenie do zmian

PISZCZ WSPÓLNICY

KANCELARIA PRAWNA

Publikacja pod redakcją radcy prawnego Mateusza Oskroby z Kancelarii Prawnej Piszcz i Wspólnicy

Autorzy:

Mateusz Oskroba, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy

Jakub Grabowski, Kancelaria Prawna Piszcz i Wspólnicy

Publikacja została przygotowana w oparciu o następujące akty prawne:

1. 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) (Dz.Urz.UE z 4 maja 2016 r. seria L 119) – zwane dalej „**RODO**",
2. ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2016 r. poz. 380 ze zm.), zwana dalej „**kc**",
3. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922) – zwana dalej **„uodo"**.

Publikacja odwołuje się również do udostępnionych w dniu 13 września 2017 roku na stronie Ministerstwa Cyfryzacji projektów: ustawy o ochronie danych osobowych oraz ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych.

Przedmiotem niniejszej publikacji jest przedstawienie zagadnienia nowych unijnych zasad dotyczących ochrony danych osobowych, związanych z wejściem w życie RODO. Niniejsza Informacja nie stanowi porady prawnej, lecz jest poglądem Autorów na przedstawianą tematykę. Kancelaria nie odpowiada za stosowanie tej publikacji w praktyce.

Poznań, dnia 30 września 2017 roku

Spis treści

Wstęp

Chcielibyśmy na wstępie uświadomić Czytelnika, że **obowiązek ochrony danych osobowych** nie jest w Polsce niczym nowym lub nadzwyczajnym. Może się to wydać zaskakujące, ale uodo obowiązuje w Polsce **od prawie 20 lat!**

Również rozwiązania przyjęte w samym RODO nie stanowią wielkiej rewolucji w zakresie ochrony danych. Niewątpliwie jednak administratorzy danych osobowych oraz organy władzy publicznej muszą się odpowiednio przygotować na dzień 25 maja 2018 roku (data, w której RODO zacznie obowiązywać), aby nowe rozwiązania, które przewiduje RODO mogły być od tego momentu skutecznie wykorzystywane.

Bardzo dużo pracy spoczywa na władzach publicznych.

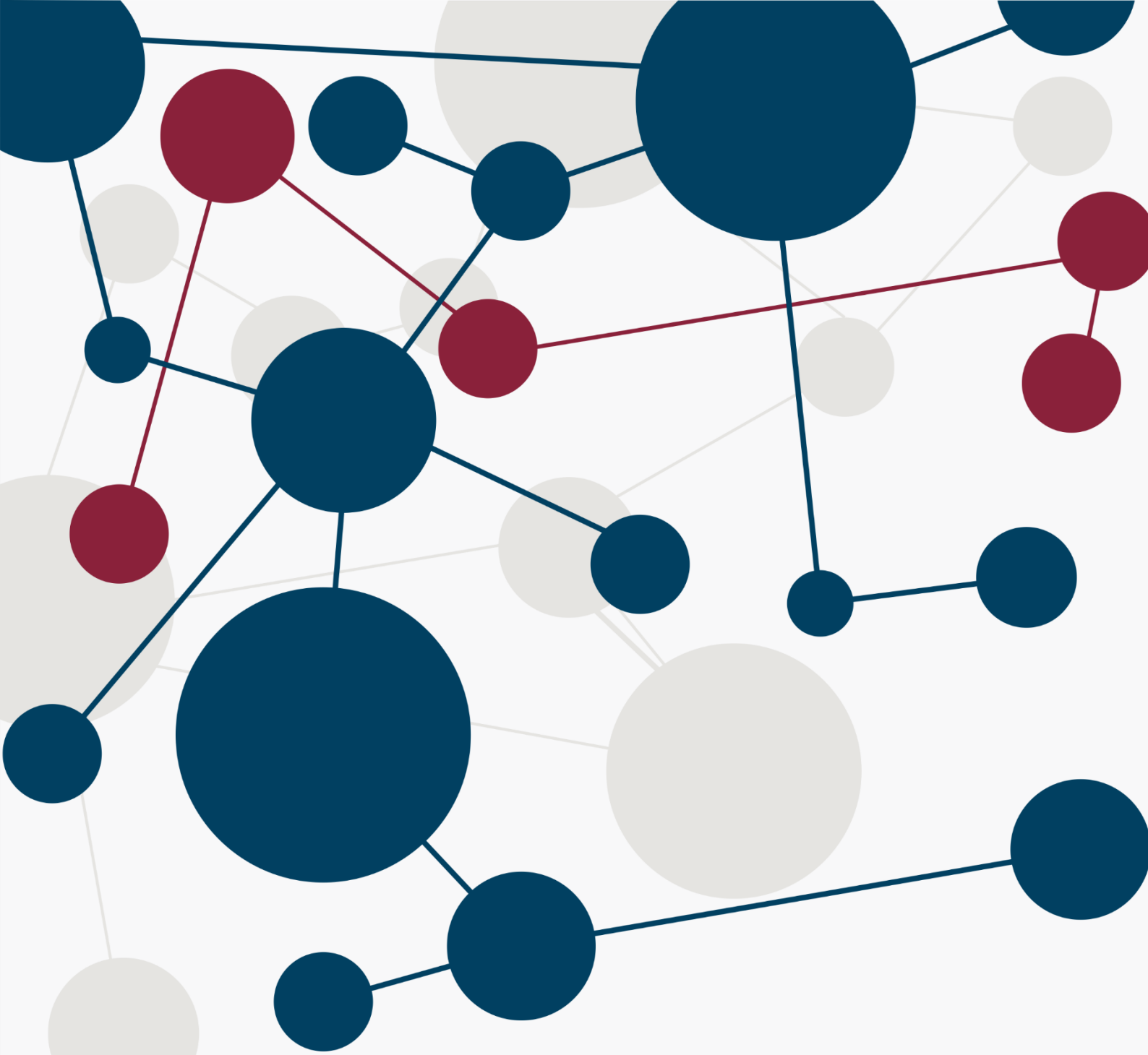
Bardzo dużo pracy spoczywa na władzach publicznych – muszą one bowiem przyjąć nową ustawę dostosowaną do RODO, dokonać przeglądu całego stanu prawnego związanego z ochroną danych i wydać odpowiednie instrukcje oraz wytyczne pozwalające stosować przepisy unijnego aktu prawnego.

Na chwilę przygotowywania niniejszej Publikacji, Ministerstwo Cyfryzacji udostępniło już projekt nowej ustawy o ochronie danych osobowych oraz projekt ustawy przepisy wprowadzające ustawę o ochronie danych osobowych. Jak można było się spodziewać projekt nowej ustawy o ochronie danych osobowych służy prawidłowemu wykonaniu RODO w ramach polskiego porządku prawnego.

Bardzo istotną kwestią jest to, że **RODO wprowadza obowiązek zapłaty kar finansowych za nieprawidłowe przetwarzanie danych osobowych**. Zagadnienie to omówione zostanie bliżej w dalszej części publikacji.

RODO wprowadza obowiązek zapłaty kar finansowych za nieprawidłowe przetwarzanie danych osobowych.

Celem Autorów jest udostępnienie Czytelnikom publikacji, która ma być dla nich pomocą w ogólnym zapoznaniu się z **zasadami dotyczącymi przetwarzania danych osobowych. Publikacja ma również wskazywać na nowe rozwiązania**, które wprowadza RODO w ochronie danych.



RODO 2018

wprowadzenie do zmian

Rozdział I

Rozdział I. **RODO – informacje ogólne**

Rozporządzenie unijne RODO (znane również pod skrótowcem GDPR) jest nowym unijnym aktem prawnym w zakresie ochrony danych osobowych. Jego celem jest jak najszersze **ujednolicenie zasad ochrony danych osobowych osób fizycznych na terenie całej Unii Europejskiej.** Ze względu na to, że rozporządzenia są unijnymi aktami prawnymi o charakterze bezpośrednio obowiązującym, to ich przepisy należy od razu stosować w państwach Unii Europejskiej bez dodatkowego uchwalania aktów prawa krajowego, które wprowadzałyby przyjęte rozwiązania. Nie oznacza to jednak, że prawodawca krajowy nie może doprecyzować niektórych ogólnych rozwiązań lub też dodać rozwiązań, których w akcie prawa unijnego brakuje. Ważne jednak, żeby takie rozwiązania były zgodne z aktem prawa unijnego oraz pozwalały bezpośrednio stosować przepisy unijne. **W konsekwencji każdy przedsiębiorca w UE zobowiązany jest bezwarunkowo przestrzegać przepisów RODO.**

Każdy przedsiębiorca w UE zobowiązany jest bezwarunkowo przestrzegać przepisów RODO.

RODO ma stanowić reakcję na szybki postęp techniczny i globalizację, co skutkuje wyraźnym upowszechnieniem zbierania, przepływu i przetwarzania informacji na coraz większą skalę.

W zakresie zastosowania przepisów znalazło się **każde przetwarzanie danych osobowych, całkowicie lub częściowo zautomatyzowane**, a także takie, które **zautomatyzowane nie jest**.

Wypada również zwrócić uwagę na wątpliwość interpretacyjną w zakresie sytuacji faktycznych, w których należy stosować przepisy RODO. Art. 2 ust. 1 RODO jest sformułowany dość niejednoznacznie w zakresie tego, czy RODO znajduje zastosowanie wyłącznie, gdy dane osobowe są lub mają być przetwarzane w zbiorze, czy też znajduje ono również zastosowanie w przypadku zautomatyzowanego przetwarzania niezależnie od tego, czy przetwarzanie następuje w zbiorze, czy też nie. **Zdaniem Autorów, uwzględniając dotychczasową wykładnię dyrektywy 95/46/WE oraz przepisy uodo, art. 2 ust. 1 RODO należy interpretować w ten sposób, że RODO znajduje również zastosowanie w przypadku przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany niezależnie od tego, czy dane te znajdują się w zbiorze danych osobowych.** Natomiast w przypadku przetwarzania w sposób inny niż zautomatyzowany, należy stosować przepisy RODO do danych osobowych, które stanowią część zbioru danych lub mają stanowić część zbioru danych.

Na potrzeby niniejszego punktu należy zwrócić uwagę na następujące definicje zawarte w RODO:

- **dane osobowe** to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[1];
- **przetwarzanie** oznacza każdą operację lub zestaw operacji wykonanych na danych osobowych lub zestawach danych osobowych – nie ma znaczenia, w jaki sposób następuje ta operacja, tzn. czy wykonuje ją człowiek, czy odbywa się ona automatycznie, przetwarzaniem danych jest również samo przechowywanie czy też niszczenie danych;
- **zbiór danych** to uporządkowany zestaw danych, dostępny na podstawie jakichś kryteriów (nie jest istotne, czy jest on scentralizowany czy zdecentralizowany lub w jakikolwiek sposób rozproszony), nawet jeżeli zbiór danych zawarty jest w analogowej formie takiej jak kartoteki, rejestr czy ewidencja – w konsekwencji nie jest możliwe „ominięcie" zbioru danych poprzez np. umieszczanie ich na różnych serwerach czy w kartotekach w różnych częściach kraju, nadal będzie to stanowić jeden zbiór.

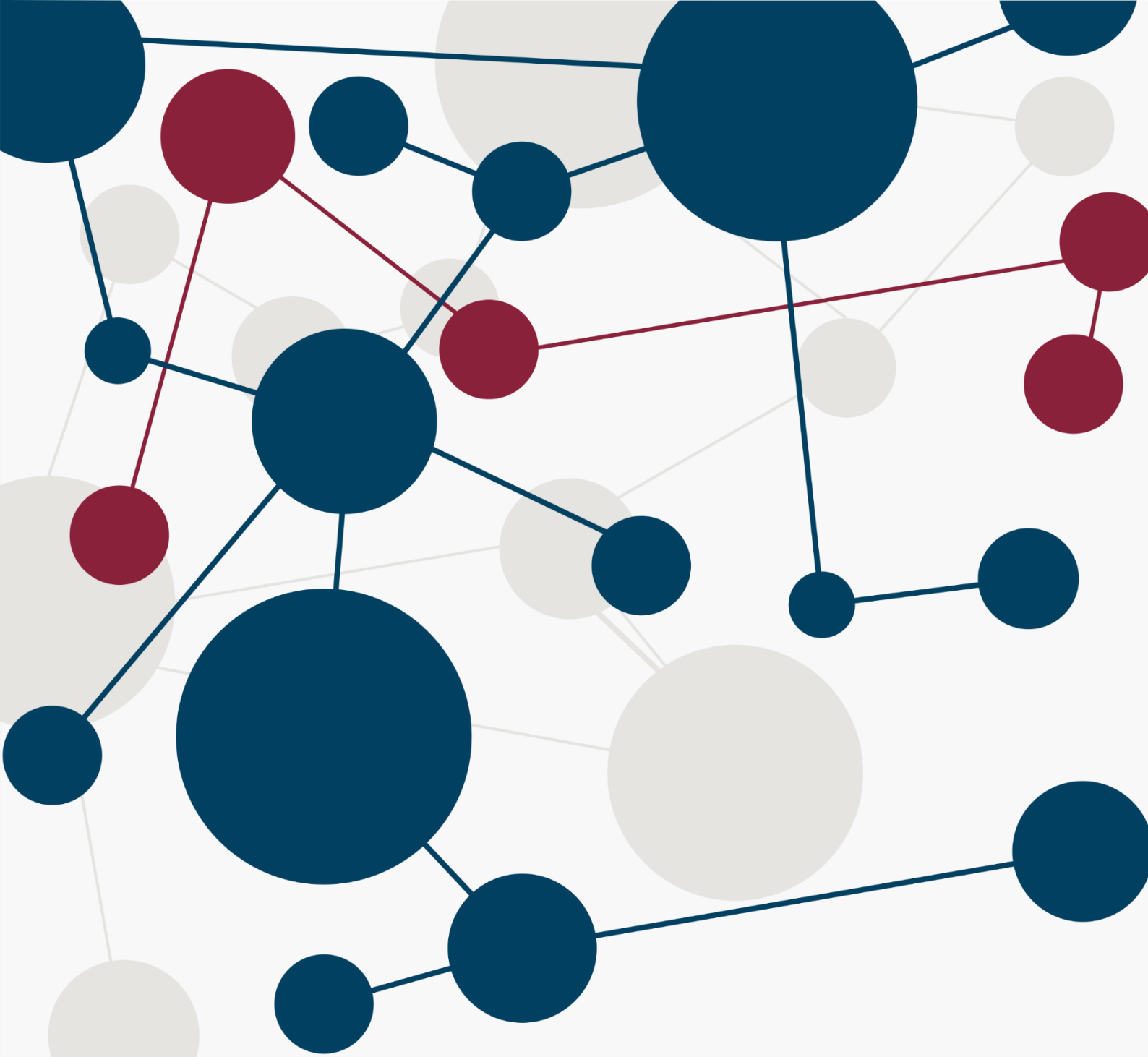
Rozporządzenie ma bardzo szeroki terytorialny zakres zastosowania. Obejmuje ono m.in. wszystkie podmioty przetwarzające dane osobowe w związku z działalnością wykonywaną w Unii Europejskiej – nawet jeżeli samo przetwarzanie nie odbywa się w Unii. **Przepisy RODO znajdą zastosowanie od 25 maja 2018 roku.**

Przykład

Przedsiębiorca XYZ S.r.l. z siedzibą w Turynie prowadzi działalność handlowo-usługową w Internecie na terenie UE. W celu optymalizacji kosztów podjęto decyzję o umieszczeniu bazy na serwerze hurtowni danych w Chinach.

Pomimo tego, że zbiór danych znajduje się poza Unią, to Spółka będzie musiała wdrożyć i stosować przepisy RODO, w tym w szczególności spełnić warunki dotyczące przekazywania danych osobowych do państwa trzeciego.

[1] Więcej na: https://biuletyn.piszcz.pl/czym-sa-dane-osobowe/ (wykorzystano 16 czerwca 2017 roku).



RODO 2018

wprowadzenie do zmian

Rozdział II

Rozdział II. **Podstawowe zasady przetwarzania danych**

RODO wymienia następujące zasady dotyczące przetwarzania danych osobowych:

1. **zasada zgodności z prawem –** zgodnie z nią każde przetwarzanie danych osobowych musi być legalne (w rozumieniu zgodności z prawem);
2. **zasada rzetelności** – choć nie została ona wyjaśniona, zasada ta zobowiązuje podmiot do dokonywania przetwarzania danych w sposób należyty, sumiennie i profesjonalnie;
3. **zasada przejrzystości** – zasada ta wymaga, aby wszelkie informacje i komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem, odnosi się to w szczególności do informowania osób, których dane dotyczą, o tożsamości administratora oraz o celach przetwarzania;
4. **zasada ograniczoności celu** – według niej zbieranie danych musi odbywać się w konkretnych, wyraźnych i prawnie uzasadnionych celach i dane te nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami;
5. **zasada minimalizacji danych** – zgodnie z tą zasadą zbieramy tylko takie dane, które są adekwatne, stosowne i ograniczone tylko do tego, co jest niezbędne do osiągnięcia celów ich przetwarzania; przykładowo daną niepotrzebną przedsiębiorcy energetycznemu do prawidłowego wykonywania umowy kompleksowej jest informacja na temat liczby posiadanych dzieci;
6. **zasada prawidłowości** – zebrane dane winny być prawidłowe (tj. zgodne z rzeczywistością) oraz uaktualniane, zasada odnosi się do celu przetwarzania – jeżeli dane są nieprawidłowe w świetle takiego celu to należy je zmodyfikować lub usunąć;
7. **zasada ograniczenia przechowywania** – przechowywanie danych osobowych dłużej, niż jest to niezbędne do osiągnięcia celów przetwarzania, jest co do zasady niedopuszczalne;
8. **zasady integralności i poufności** – zobowiązują one do zapewnienia bezpieczeństwa danych osobowych, w szczególności przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (naruszenie poufności), przypadkową utratą, zniszczeniem lub uszkodzeniem (naruszenie integralności);
9. **zasada rozliczalności** – zobowiązuje administratora do tego, aby był w stanie wykazać przestrzeganie wszystkich powyższych zasad.

1. Osoba odpowiedzialna za przetwarzanie danych

Według przepisów RODO to administrator jest odpowiedzialny za przetwarzanie danych osobowych.

Administrator jest odpowiedzialny za przetwarzanie danych osobowych.

Administrator to osoba fizyczna lub prawna, organ publiczny, **jednostka lub inny podmiot**, który samodzielnie lub wspólnie z innymi **ustala cele i sposoby przetwarzania danych osobowych**.

Administratorem jest zatem ten podmiot (niezależnie od jego formy prawnej), który **decyduje o tym, jak i po co dane osobowe będą przetwarzane.** Z uwagi na użyte w RODO określenie „jednostka lub inny podmiot" nie ma wątpliwości, że definicją tą objęte są również jednostki nieposiadające osobowości prawnej, którym właściwe przepisy przyznają zdolność prawną (czyli m. in. osobowe spółki prawa handlowego).

Skoro więc administrator decyduje o **sposobach** przetwarzania, to musi on zadbać o to, aby sposoby, zarówno techniczne, jak i organizacyjne **były zgodne z zasadami przetwarzania danych, o których mowa powyżej.**

W zakresie środków organizacyjnych należy przykładowo pamiętać, aby **odpowiednio przeszkolić pracowników**, którzy mają styczność z danymi osobowymi pod kątem zasad ich ochrony.

W zakresie środków organizacyjnych należy pamiętać, aby odpowiednio przeszkolić pracowników.

Biorąc pod uwagę środki techniczne (szczególnie z uwzględnieniem odesłań RODO do nowych technologii i informatyzacji życia) należy przykładowo zwrócić uwagę na wirtualne zbiory danych osobowych (ogólniej – elektroniczne bazy danych) przetwarzane z wykorzystaniem sprzętu komputerowego. Takie bazy danych są szczególnie narażone na różnego rodzaju naruszenia ich bezpieczeństwa, skutkujące utratą kontroli administratora nad danymi. W konsekwencji w celu zapewnienia bezpieczeństwa **administrator musi wprowadzić odpowiednie zabezpieczenia sprzętowe – typu hardware** (np. zwrócenie uwagi, jak podłączone do sieci są serwery), jak i zabezpieczenia programowe – **typu software** (np. korzystanie z programów antywirusowych, dostępnych firewalli).

2. Od jakiego momentu należy stosować przepisy RODO?

Przepisy **RODO należy stosować jeszcze przed rozpoczęciem przetwarzania danych osobowych w systemach informatycznych** (lub jakiejkolwiek innej formie zautomatyzowanego bądź częściowo zautomatyzowanego przetwarzania danych) **lub w zbiorach** (w przypadku przetwarzania innego niż zautomatyzowane).

Przepisy RODO należy stosować jeszcze przed rozpoczęciem przetwarzania danych osobowych.

Wynika to z faktu, że przetwarzanie danych osobowych powinno odbywać się w bezpiecznych warunkach lub też w warunkach, które umożliwiają ich przetwarzanie zgodnie z prawem. RODO określa to jako ochrona danych w fazie projektowania (*privacy by design).* Jeżeli więc administrator planuje przetwarzanie danych osobowych, ustalając

cele przetwarzania, to już na etapie projektowania systemu powinien on wdrożyć rozwiązania zgodne z RODO. **W przeciwnym wypadku rozpocznie przetwarzanie niezgodnie z omawianym aktem prawnym.**

Natomiast faktycznie zasady dotyczące przetwarzania danych osobowych zawarte w RODO znajdą najszybciej zastosowanie z chwilą, gdy podmiot wejdzie w posiadanie danych osobowych, które ma zamiar umieścić w zbiorze lub które już stanowią część zbioru danych.

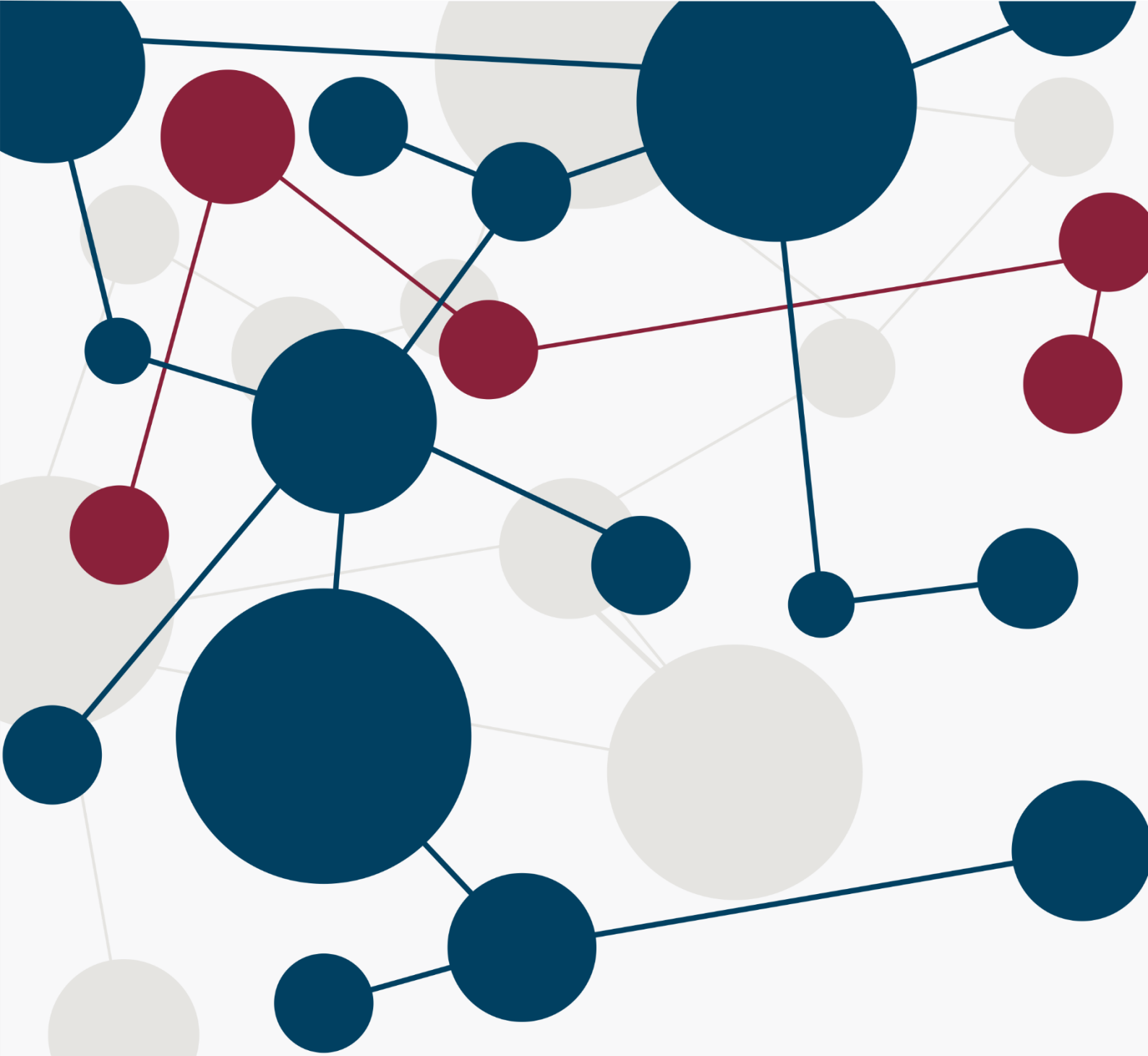
W przypadku danych znajdujących się już w zbiorze sytuacja jest jasna – jeżeli dana jest w nim umieszczona, to należy stosować RODO. **W jaki sposób należy natomiast rozumieć sytuację, w której dane mają dopiero stanowić część zbioru?**

Przykład

Przedsiębiorca XYZ S.A. zajmuje się wysyłkową sprzedażą towarów. Zamówienia przyjmowane są drogą elektroniczną lub za pomocą specjalnych, papierowych formularzy zamieszczonych w poczytnym tygodniku, na którym zamawiający podaje swoje dane oraz wybiera produkt, a następnie pakuje ten formularz do koperty i wysyła do przedsiębiorcy.

W przypadku zamówienia elektronicznego, dane przesłane przez klienta zapisywane są automatycznie w bazie danych klientów (potencjalnych klientów) Spółki. Każda operacja na nich wykonana polegać będzie regulacjom RODO.

Co zatem z zamówieniem złożonym przy pomocy zwykłej korespondencji? Oczywistym jest, że gdy do siedziby Spółki wpłynie korespondencja, w której znajduje się zamówienie to nie stanowi ona automatycznie części zbioru danych – musi być wpierw przetworzona, żeby trafić do takiego zbioru, czyli zostać wprowadzona do bazy danych Spółki. Nie zmienia to jednak statusu danych zawartych w takim zamówieniu, które już od chwili wpłynięcia ich do Spółki podlegają ochronie przewidzianej w RODO.



RODO 2018

wprowadzenie do zmian

Rozdział III

Rozdział III. **Podstawy prawne umożliwiające przetwarzanie danych osobowych**

Tak jak w przypadku uodo, RODO dzieli dane osobowe na dwie grupy:

- szczególne kategorie danych osobowych (tzw. dane wrażliwe) oraz
- dane osobowe jako takie.

RODO określa podstawy prawne umożliwiające przetwarzanie zarówno wrażliwych danych osobowych, jak i „zwykłych" danych osobowych.

RODO określa podstawy prawne umożliwiające przetwarzanie zarówno wrażliwych danych osobowych, jak i „zwykłych" danych osobowych.

1. Podstawy przetwarzania „zwykłych" danych osobowych

RODO stanowi, że można przetwarzać zwykłe dane osobowe w następujących przypadkach:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (zgoda na przetwarzanie);
- przetwarzanie jest niezbędne do wykonania umowy z osobą, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (wykonanie umowy);
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (obowiązek wynikający z przepisów prawa);
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej (żywotne interesy osoby);
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (interes publiczny, sprawowanie władzy publicznej);
- 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 (prawnie uzasadniony interes).

Punkty trzeci i piąty winny być dookreślone w przepisach prawa Unii Europejskiej lub przepisach prawa państwa członkowskiego. Innymi słowy punkty te

muszą mieć swoje odzwierciedlenie w innych przepisach prawa – same w sobie nie powinny stanowić wyłącznej podstawy prawnej do przetwarzania danych.

Należy też zaznaczyć, że **punkt czwarty** co do zasady powinien stanowić podstawę do przetwarzania danych osoby, której one dotyczą wyłącznie w przypadku, gdy administrator nie będzie mógł oprzeć się na innej podstawie przetwarzania tych danych.

Punkt szósty nie ma jednak zastosowania do przetwarzania danych osobowych przez organy publiczne.

Należy mieć na uwadze, że każda z tych podstaw jest samodzielną przesłanką do przetwarzania danych osobowych (z uwzględnieniem kwestii poruszonych w niniejszym punkcie).

Jeżeli przetwarzanie danych osobowych jest niezbędne do realizacji umowy, to nie jest nam dodatkowo potrzebna zgoda osoby.

Jeżeli więc administrator wykaże, że przetwarzanie danych osobowych jest niezbędne do realizacji umowy, to nie jest nam dodatkowo potrzebna zgoda osoby, której dane dotyczą na przetwarzanie tych danych.

2. Zgoda na przetwarzanie danych osobowych i wyjątek dotyczący dzieci

Odnosząc się do przesłanki zgody na przetwarzanie danych osobowych, należy wskazać, że **RODO określa warunki**, które są niezbędne, aby wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych.

Przez **zgodę** RODO rozumie **dobrowolne**, **konkretne**, **świadome** i **jednoznaczne okazanie woli**, w którym osoba, której dane dotyczą, w formie **oświadczenia** lub **wyraźnego działania potwierdzającego**, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Przepisy RODO kładą istotny nacisk na dobrowolność udzielanej zgody, wskazując, że w sytuacji, w której istnieje wyraźny brak równowagi między administratorem a osobą, której dane dotyczą, jest mało prawdopodobne, aby zgoda była wyrażona dobrowolnie.

Administrator zobowiązany jest wykazać wyrażenie zgody przez osobę, której dane dotyczą.

Dodatkowo RODO przewiduje, że to na administratorze ciążą następujące obowiązki w zakresie pozyskiwania zgody:

- **administrator zobowiązany jest wykazać wyrażenie zgody przez osobę**, której dane dotyczą,

- jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o **zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić to zapytanie od pozostałych kwestii** – zatem często spotykane w ogólnych warunkach umów dodawanie postanowień o zgodach na inne cele przetwarzania danych niż wykonanie umowy, na które to cele osoba podpisująca umowę niejako godzi się, akceptując postanowienia umowy – jest niedopuszczalne.

Drugi obowiązek może również stanowić argument za tym, **aby nie łączyć różnych celów a nawet sposobów przetwarzania danych w jeden formularz zgody**, który można w całości zaakceptować albo w całości odrzucić. W najbardziej abstrakcyjnym scenariuszu interpretacyjnym na każdą operację na danych osobowych trzeba będzie uzyskiwać odrębną zgodę. W takim wypadku należałoby pozyskiwać odrębną zgodę na przechowywanie danych w celu przygotowania oferty handlowej, odrębną w celu wykorzystania danych do przygotowania oferty a nawet odrębną zgodę w celu zebrania danych osobowych i włączenia ich do zbioru danych marketingowych. Uważamy jednak, że bezpiecznym **rozwiązaniem będzie pozyskiwanie zgody dla jednego celu przetwarzania, który ogranicza się do jednego administratora, ewentualnie do współadministratorów.**

Istotna regulacja została wprowadzona w stosunku do danych osobowych dzieci. Zgodnie z postanowieniami RODO **dziecko** do szesnastego roku życia **nie może samodzielnie wyrazić zgody** na przetwarzanie jego danych osobowych **bez jednoczesnej zgody rodzica lub opiekuna prawnego**.

> Dziecko do szesnastego roku życia nie może samodzielnie wyrazić zgody na przetwarzanie jego danych osobowych.

Zgodnie z RODO **granica wiekowa może zostać obniżona do trzynastego roku życia** przez ustawodawstwo państwa członkowskiego – **z czego najprawdopodobniej skorzysta Polska**, gdyż w projekcie nowej ustawy o ochronie danych osobowych przewiduje się, że zgoda rodziców lub opiekunów prawnych osoby, która nie ukończyła trzynastu lat, jest wymagana, jeżeli przetwarzanie opiera się na zgodzie osoby, której dane dotyczą.

3. Podstawy prawne przetwarzania danych wrażliwych

Przez **dane wrażliwe** należy rozumieć dane ujawniające **pochodzenie rasowe** lub **etniczne**, **poglądy polityczne**, **przekonania religijne** lub **światopoglądowe**, **przynależność do związków zawodowych** oraz **dane genetyczne**, **dane biometryczne** w celu jednoznacznego zidentyfikowania osoby fizycznej lub **dane dotyczące zdrowia**, **seksualności** lub **orientacji**.

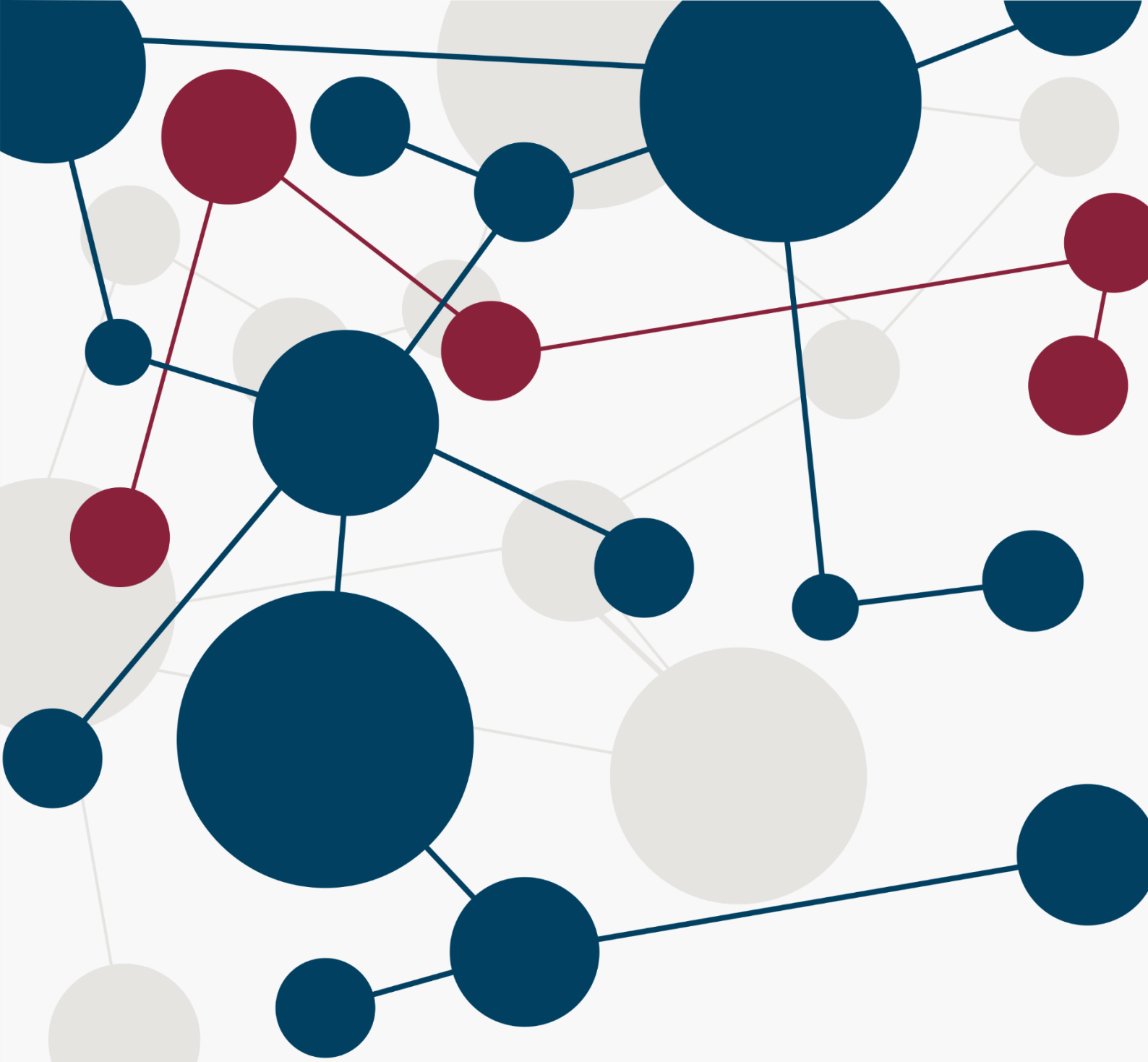
Generalna zasada wysłowiona w RODO stanowi, że zabrania się przetwarzania danych osobowych będących danymi wraż-

liwymi. Jednakże przepisy RODO przewidują **enumeratywny katalog przesłanek,** na podstawie których **przetwarzanie takich danych jest jednak dopuszczalne** (art. 9 RODO). Najważniejsze z nich to:

- udzielenie wyraźnej zgody na przetwarzanie tych danych, zgoda musi wskazywać konkretny cel lub cele tego przetwarzania, nie można zatem skonstruować takiej klauzuli, która pozwoliłaby na swobodę w przetwarzaniu – jeżeli osoba zgodzi się na przetwarzanie swoich danych wrażliwych w jednym, ściśle określonym celu to niedopuszczalne będzie „rozszerzanie" zgody na inne cele w drodze jej kreatywnej interpretacji;
- nałożenie prawnego obowiązku na administratora wykonywania szczególnych zobowiązań w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, z punktu widzenia przedsiębiorcy będzie to szczególnie dotyczyło m. in. dokumentacji pracowniczej;
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej, medycyny pracy, oceny zdolności pracownika do pracy oraz celów związanych z zapewnianiem zinstytucjonalizowanej opieki zdrowotnej, w konsekwencji zakłady opieki zdrowotnej nie potrzebują specjalnych zgód czy innych oświadczeń od pacjentów do przetwarzania danych dotyczących ich zdrowia.

Nie są to oczywiście wszystkie przesłanki (jest ich jeszcze siedem), jednak z punktu widzenia prowadzenia biznesu są one najbardziej istotne.

W kontekście pojawiającego się często przy zatrudnianiu pracowników wymogu przedłożenia zaświadczenia z Krajowego Rejestru Karnego RODO nie przesądza wprost o dopuszczalności bądź nie. Odsyła za to do zgodności z przepisami unijnymi bądź wewnętrznymi przepisami państwa członkowskiego.



RODO 2018

wprowadzenie do zmian

Rozdział IV

Rozdział IV. **Prawa osób, których dane dotyczą**

W zakresie praw, które przysługują osobom, których dane dotyczą oraz obowiązków informacyjnych, ciążących na administratorach danych, RODO przewiduje szereg zasad ogólnych, którymi musi kierować się administrator danych. Wprowadzenie tych zasad należy uznać za realizację **zasady przejrzystości** (s. 10).

1. Ogóle zasady informowania i komunikacji z osobami, których dane dotyczą

Przede wszystkim są to **wymagania dotyczące języka i formy.** Wszelkie informacje udzielane osobom oraz wszelka komunikacja z osobami, których dane dotyczą, muszą być **zwięzłe**, **krótkie**, **przejrzyste**, **zrozumiałe** oraz zawarte w **łatwo dostępnej formie**, natomiast język musi być **jasny** i **prosty**. Mają być udzielone **na piśmie lub w inny sposób** (w stosownych przypadkach elektronicznie).

Wszelkie informacje oraz komunikaty muszą być zwięzłe, krótkie, przejrzyste i zrozumiałe.

Za niezgodne z przepisami RODO trzeba będzie więc uznać udzielanie informacji lub komunikację w takiej formie, która będzie niezrozumiała dla przeciętnego człowieka, np. zawierając w tekście dużo skomplikowanego słownictwa.

Administrator obowiązany jest do ułatwienia korzystania z praw przysługującym osobom.

Ponadto, **administrator obowiązany jest do ułatwiania korzystania z praw przysługujących osobom.** Musi on więc powziąć takie środki, aby rzeczywiście osoba mogła w sposób wolny od utrudnień uzyskiwać informacje oraz wykonywać swoje prawa (o prawach będzie mowa w dalszej części niniejszej Informacji, s. 21).

RODO określa również **termin**, w jakim administrator powinien udzielić odpowiedzi na kierowane do niego żądania. Zasadą jest odpowiedź **bez zbędnej zwłoki** – **jednakże nie dłużej niż jeden miesiąc** (z możliwością przedłużenia o **dwa kolejne miesiące**, gdy żądanie ma skomplikowany charakter lub tych żądań jest tak dużo, że niemożliwym byłoby zrealizowanie ich wszystkich w podstawowym terminie). Jeżeli natomiast administrator stwierdza brak podstaw do podjęcia działań w związku z żądaniem to **niezwłocznie** (jednak nie dłużej niż w ciągu miesiąca) udziela informacji zwrotnej ze wskazaniem przyczyn niepodjęcia działań.

Udzielanie informacji oraz realizacja praw muszą być co do zasady bezpłatne.

Administratorowi przysługuje prawo do tego, aby żądać dodatkowych informacji o osobie kierującej do niego żądanie w celu właściwego zidentyfikowania osoby, której dane dotyczą.

Udzielanie informacji oraz realizacja praw muszą być co do zasady bezpłatne.

Powyższe zasady **stosuje się do wszystkich obowiązków informacyjnych oraz relacji administrator-osoba przy realizacji jej praw.**

2. Obowiązki informacyjne administratora

Podobnie jak w przypadku obecnie obowiązującej ustawy, RODO rozróżnia obowiązki informacyjne w zależności od sposobu pozyskania danych osobowych – poprzez zebranie danych od osoby, której dane dotyczą oraz pozyskanie danych od innej osoby niż osoba, której dane dotyczą (art. 24 i 25 uodo).

Według rozwiązań przyjętych przez RODO w zakres obowiązków informacyjnych **w przypadku zbierania danych od osoby, której dane dotyczą,** wchodzi:

- podanie swojej tożsamości i danych kontaktowych, w przypadku osób prawnych będzie zatem chodziło o nazwę (firmę), dokładny adres siedziby, podanie numeru kontaktowego czy adresu poczty elektronicznej itp.;
- podanie, w przypadku, gdy administrator ustanowi inspektora danych osobowych – danych tego inspektora, w RODO inspektor danych osobowych jest odpowiednikiem ABI ustanawianego na podstawie uodo (o inspektorze będzie mowa w dalszej części publikacji);
- podanie celu przetwarzania oraz podstawy prawnej przetwarzania;
- podanie, jeżeli do przetwarzania dochodzi w celu realizacji prawnie uzasadnionych interesów administratora, tych prawnie uzasadnionych interesów;
- podanie informacji o odbiorcach danych osobowych lub kategoriach odbiorców (przez odbiorcę danych rozumie się te podmioty, którym dane są ujawniane);
- określenie okresu, przez który dane będą przetwarzane lub, gdy to niemożliwe, określenie kryterium ustalania takiego okresu;
- poinformowanie osoby o przysługujących jej prawach (o których będzie mowa dalej):
    - prawie do cofnięcia zgody na przetwarzanie danych,
    - prawie do sprostowania danych,
    - prawie do dostępu do swoich danych,
    - prawie do żądania usunięcia danych,
    - prawie do żądania ograniczenia przetwarzania danych,
    - prawie do wniesienia sprzeciwu wobec przetwarzania danych,
    - prawie do przenoszenia danych;
- poinformowanie o przysługującym prawie do wniesienia skargi do organu nadzorującego przetwarzanie danych osobowych;
- informacja o tym, czy przetwarzanie danych jest wymagane ustawą, umową bądź jest warunkiem koniecznym do zawarcia umowy, czy dana osoba jest

zobowiązana do ich podania oraz o tym, jakie są konsekwencje ich niepodania;
- przekazanie informacji o tym, czy dane będą służyć do zautomatyzowanego podejmowania decyzji, w tym profilowania oraz zasad, według których będzie się to odbywać.

Jak więc widać, katalog informacji jest niezwykle szeroki i stosowanie się do niego ciąży na każdym administratorze.

Z obowiązku informacyjnego administrator zwolniony jest tylko w takim zakresie, w jakim osoba, której dane dotyczą jest już w posiadaniu informacji.

Przykład

Klient zakłada konto na platformie www.xyz.pl, prowadzonej przez Jana Kowalskiego. Podczas rejestracji podawał swoje imię, nazwisko oraz adres, pod którym prowadzi swoją działalność gospodarczą. Przy zakładaniu konta dostępny jest dokument, w którym podane są wszystkie konieczne informacje.

Platforma xyz.pl po czasie zaczęła oferować nowe usługi, do których wykonania niezbędny jest adres zamieszkania Klienta. Klient, decydując się na korzystanie z tych nowych usług, wprowadza do systemu dodatkowe dane dotyczące swojej osoby. W takim wypadku prowadzący portal Jan Kowalski nie będzie zobowiązany do identyfikacji swojej osoby oraz nie powinien być ponownie zobowiązany do informowania Klienta o danych kontaktowych inspektora ochrony danych, jeżeli nie uległy one zmianie.

Obowiązek informacyjny **w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą**, jest poszerzony względem wyżej przedstawionego o wskazanie:

- **kategorii odnośnych danych osobowych**, czyli kategorie, do których dane należą, np. dane klientów, dane pracowników, dane adresatów działań marketingowych;
- **źródła pochodzenia danych osobowych** (w przypadku danych pochodzących ze źródeł publicznie dostępnych należy o tym również poinformować).

Zwolnienie z obowiązku informacyjnego w tym przypadku zachodzi dodatkowo m. in. w sytuacji, gdy **udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.**

3. Prawo dostępu

Osoba, której dane dotyczą ma **prawo dostępu** do swoich danych osobowych. Przepisy RODO (art. 15) nie przewidują ograniczenia tego prawa ani w czasie, ani co do osób uprawnionych.

Po pierwsze, każdej osobie przyznane jest prawo skierowania do administratora pytania, **czy jej dane osobowe są przez niego przetwarzane.** Jeżeli są, to należy umożliwić do nich dostęp, oraz udzielić na żądanie następujących informacji o:

- celu przetwarzania;
- kategoriach odnośnych danych osobowych;
- odbiorcach lub kategoriach odbiorców danych, którym dane osobowe są lub będą udostępnione;
- planowanym okresie przechowywania danych lub kryteriach ustalania takiego okresu;
- prawie wniesienia skargi do organu nadzorczego;

- źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą;
- zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Administrator ma również obowiązek **udostępnić kopię danych podlegających przetwarzaniu.**

Administrator ma obowiązek udostępnić kopię danych podlegających przetwarzaniu.

4. Prawo sprostowania danych

Jeżeli dane osoby są przetwarzane w zbiorze przez administratora, osoba ta ma prawo żądać **sprostowania danych,** czyli „dopasowania" treści danych do stanu rzeczywistego.

Administrator nie może odmówić realizacji prawa do sprostowania danych.

Co więcej – jeżeli cele przetwarzania wymagają większej ilości danych niż ta, która jest w posiadaniu administratora (np. potrzebny jest jeszcze adres zamieszkania, czego w zbiorze nie ma), osoba ma prawo **uzupełnić** swoje dane o te, które są konieczne.

Administrator nie może odmówić realizacji tego prawa.

5. Prawo do usunięcia danych („prawo do bycia zapomnianym")

„Prawo do bycia zapomnianym" jest pojęciem już obecnym w prawie Unii Europejskiej. Odnosi się do wyroku TSUE z 2014 r.[2] Jeszcze na podstawie dyrektywy 95/46/WE Trybunał uznał, że każdemu przysługuje **„prawo do bycia zapomnianym w Internecie"** co oznaczało, że można było **żądać usunięcia swoich danych** z wyszukiwarki internetowej (odnosiło się to tylko do imienia i nazwiska).

Uprawnienie określone w RODO jest w istocie **poszerzonym prawem do żądania usunięcia danych osobowych**.

Po pierwsze – można żądać **usunięcia swoich danych osobowych ze zbioru, gdy:**

- dane nie są już niezbędne do celów, w których zostały zgromadzone, przepis przewiduje brak niezbędności, a nie zbędność – oznacza to, że jeżeli można obejść się bez tych danych do realizowania celów, dla których zostały zebrane (choćby i były przydatne), to należy je na żądanie usunąć;
- zostanie wycofana zgoda na przetwarzanie, a nie ma innej podstawy prawnej do przetwarzania;
- osoba wniesie sprzeciw wobec przetwarzania niezbędnego do wykonania zadań publicznych lub

[2] Sygnatura C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi.

wykonywania władzy publicznej oraz w celu realizacji prawnie uzasadnionych interesów administratora i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
- osoba wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane muszą być usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie UE lub państwa członkowskiego, któremu podlega administrator;
- dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego (czyli odpłatnych usług, świadczonych na odległość drogą elektroniczną) dziecku poniżej 16 roku życia.

Elementem, który jest bardzo istotny w porównaniu do uodo jest **obowiązek podjęcia kroków przez administratora, który upublicznił dane do tego, aby inni administratorzy przetwarzający te dane również je usunęli.**

Jednakże nie można żądać usunięcia danych i „bycia zapomnianym" m.in. gdy przetwarzanie **jest konieczne do realizacji prawnie nałożonych obowiązków** oraz **do ustalenia, dochodzenia lub obrony roszczeń.**

Przykład

Przedsiębiorca XYZ sp. j. jest administratorem zbioru danych swoich klientów, które wykorzystuje do świadczenia swoich usług. Zbiór jest bardzo obszerny i oprócz podstawowych danych, takich jak imię, nazwisko czy adres przechowywane są dodatkowe, spersonalizowane informacje, zgromadzone w toku stałego świadczenia usług.

Klient, mając u Spółki 100 000 zł zadłużenia z tytułu nieopłaconych faktur, chcąc uniknąć odpowiedzialności, żąda usunięcia swoich danych i „zapomnienia".

Spółka w naszej ocenie powinna usunąć tylko te dane, które nie są jej niezbędne do ustalenia oraz dochodzenia roszczeń przeciwko takiemu Klientowi. Pozostałe dane takie jak imię, nazwisko, adres, numer PESEL, potrzebne do wytoczenia powództwa, będą mogły pozostać w zbiorze.

6. Prawo do ograniczenia przetwarzania

Nową, w stosunku do uodo, instytucją jest **prawo do ograniczenia przetwarzania.** Ograniczenie przetwarzania polega na tym, że w przypadku jego zastosowania administrator może przetwarzać dane wyłącznie za zgodą osoby, której te dane dotyczą. Zgoda na przetwarzanie nie jest natomiast wymagana do przechowywania takich danych oraz sytuacji, w których przetwarzanie jest konieczne do ustalenia, dochodzenia lub obrony roszczeń, bądź też w celu ochrony praw osoby fizycznej.

Żądać ograniczenia można, gdy:

- kwestionuje się prawidłowość danych osobowych – na czas potrzebny do weryfikacji ich prawidłowości;
- przetwarzanie jest niezgodne z prawem, lecz osoba, której dane dotyczą, sprzeciwia się usunięciu i żąda w zamian ograniczenia przetwarzania;
- administrator nie potrzebuje już danych, lecz są one potrzebne osobie, której

dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- osoba zgłosi sprzeciw wobec przetwarzania – do czasu rozpatrzenia sprzeciwu.

Mając powyższe na uwadze, prawo ograniczenia przetwarzania przypomina środek tymczasowy, który może zostać zastosowany przez osobę, której dane dotyczą, w celu zabezpieczenia swoich interesów w okresie analizy sprawy przez administratora danych.

7. Prawo do przenoszenia danych

Również interesującą nowością w ramach RODO jest wprowadzenie prawa do przenoszenia danych. Zgodnie z nim osoba, której dane dotyczą ma prawo żądać otrzymania danych osobowych jej dotyczących w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego oraz ma prawo przekazać te dane innemu administratorowi **bez przeszkód ze strony pierwotnego administratora.**

Oznacza to, że administrator, który pozyskał dane osobowe osoby fizycznej, **nie może mieć „monopolu" na ich przetwarzanie.**

Prawo do przenoszenia obejmuje sytuacje, gdy przetwarzanie oparte jest **na zgodzie** lub **w celu wykonania umowy** i **odbywa się w sposób zautomatyzowany.**

Ponadto, w ramach prawa do przenoszenia danych, osoba może żądać, aby pierwotny administrator przesłał dane bezpośrednio innemu administratorowi, jeżeli jest to technicznie możliwe. W dobie informatyzacji życia trudno wyobrazić sobie sytuację, w której nie istniałaby techniczna możliwość spełnienia tego obowiązku.

Odpowiadając na pytanie, czy administratorzy, którzy przygotowują takie informacje, mogą żądać stosownego wynagrodzenia w tym zakresie, należy wskazać, że w zasadzie obowiązek uczynienia zadość prawu do przenoszenia danych powinien być realizowany nieodpłatnie, na co już zwracaliśmy uwagę w punkcie VII.1. powyżej.

8. Prawo do sprzeciwu

Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw przeciwko przetwarzaniu jej danych osobowych.

Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw przeciwko przetwarzaniu jej danych osobowych.

Efektem wniesienia skutecznego sprzeciwu jest niedopuszczalność dalszego przetwarzania danych tej osoby (z pewnym ograniczeniem, o czym dalej).

Wniesienie sprzeciwu może nastąpić w przypadku, gdy:

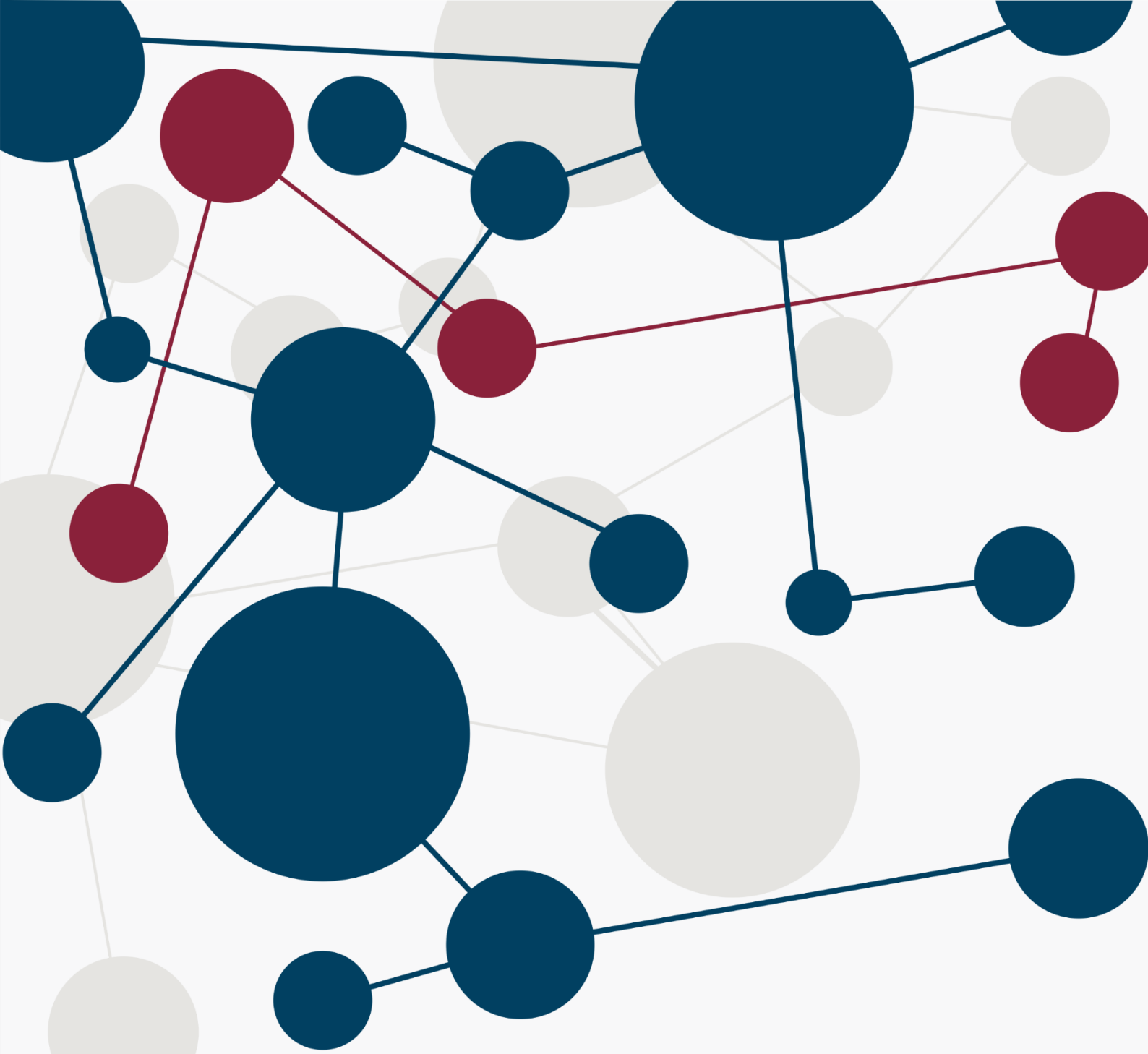
- przetwarzanie odbywa się w związku realizacją zadań publicznych i władzy publicznej,
- w celu realizowania prawnie uzasadnionych interesów administratora.

Sprzeciw można zgłosić z przyczyn związanych ze szczególną sytuacją osoby, której dane dotyczą. Dalsze przetwarzanie

będzie dopuszczalne tylko wtedy, gdy wykazany zostanie istniejący, ważny, prawnie uzasadniony interes administratora danych, nadrzędny względem interesów osoby, której dane dotyczą.

Jeżeli jednak administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, osoba składająca sprzeciw nie musi legitymować się żadną szczególną sytuacją, aby administrator był zobowiązany do zaprzestania przetwarzania w tym celu.

Należy zauważyć, że RODO wymaga **osobnego, jasnego poinformowania osoby, której dane dotyczą o przysługującym jej uprawnieniu do złożenia sprzeciwu.**



RODO 2018

wprowadzenie do zmian

Rozdział V

Rozdział V. **Profilowanie**

Profilowanie stanowi operację przetworzenia (wykonywaną bez udziału człowieka) danych początkowych dotyczących osoby fizycznej przy wykorzystaniu pewnych założeń początkowych celem uzyskania określonego wniosku końcowego, który powinien dotyczyć tej osoby.

1. Pojęcie profilowania w RODO

Profilowanie oznacza **dowolną formę 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, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

> Profilowanie służy często do podejmowania decyzji, które wywołują skutki prawne wobec osoby lub mogą takie skutki wywoływać.

Istotną kwestią w zakresie profilowania nie jest sam proces profilowania tylko jego wynik. RODO zwraca uwagę na profilowanie, albowiem służy ono **często do podejmowania decyzji, które wywołują skutki prawne wobec osoby lub mogą takie skutki wywoływać**, bądź też podobnie istotnie wpływać na tę osobę**.** Profilowanie jest również wykorzystywane w marketingu, gdyż ułatwia precyzyjne kierowanie określonych działań promocyjnych do osób, które mogą być nimi zainteresowane**.**

2. Przykłady profilowania

Do profilowania dochodzi w wielu dziedzinach gospodarki i jest to zjawisko coraz częstsze. **Przykładowo, profilowanie stosuje się w:**

- bankowości;

Przykład

Klient detaliczny banku korzysta z aplikacji mobilnej, która umożliwia wzięcie błyskawicznej pożyczki. Bank, obsługując rachunek klienta ma dostęp do jego danych osobowych, w tym takich danych jak dochody oraz wydatki.

Mając dostęp do tych informacji, system sam wylicza zdolność kredytową i bez ingerencji człowieka zezwala na wzięcie pożyczki w takiej a nie innej kwocie.

- marketing bezpośredni;

Przykład

Przedsiębiorca dostarcza usługi telefonii komórkowej. Klient, posiadający numer w tej sieci regularnie wyjeżdża służbowo na Ukrainę. Operator ma informacje dotyczące położenia telefonu swojego klienta i system

„zauważa", że w logowaniu na Ukrainie występuje pewna regularność.

Przetwarzając dane na potrzeby akcji promocyjnej nowej usługi, polegającej na nielimitowanych rozmowach i powiększonym pakiecie internetowym na terenie Ukrainy, system „wyrzuca" tego klienta jako potencjalnie zainteresowanego nową usługą, w związku z czym operator dzwoni do klienta, starając się namówić go na zakup nowego pakietu.

- ubezpieczenia;

Przykład

Przedsiębiorca działa w obszarze produktów ubezpieczeniowych. Gromadzi on historię ubezpieczeniową osoby – rodzaje wykupywanych wcześniej ubezpieczeń, częstotliwość zgłaszania zdarzeń ubezpieczeniowych, wysokości wypłacanych świadczeń itp.

Gdy klient przychodzi do placówki ubezpieczyciela w celu wykupienia ubezpieczenia na wyjazd wakacyjny, to system informatyczny samodzielnie wylicza wysokość proponowanych składek, zakres możliwej do udzielenia ochrony ubezpieczeniowej, uwzględniając poziom ryzyka na podstawie informacji o kliencie.

3. Warunki dotyczące profilowania

Warto zauważyć, że profilowanie podlega w RODO pewnym dodatkowym wymogom ciążącym na administratorze danych. Zgodnie z postanowieniami RODO:

- gdy dochodzi do zautomatyzowanego podejmowania decyzji, w tym profilowania, konieczne jest poinformowanie osoby, której dane dotyczą, że będą przetwarzane w ten sposób oraz o konsekwencjach profilowania (co do obowiązków informacyjnych – s. 20);
- w odniesieniu do profilowania realizowanego na potrzeby marketingu bezpośredniego osobie, której dane dotyczą, przysługuje nieskrępowane prawo do sprzeciwu w zakresie takiego przetwarzania.

4. Zautomatyzowane podejmowanie decyzji na podstawie profilowania jako szczególny przypadek przetwarzania danych w RODO

Ze względu na to, że profilowanie odbywa się w sposób zautomatyzowany, bez udziału czynnika ludzkiego, ustawodawca unijny zadecydował, że w przypadku, gdy skutkiem profilowania jest również automatyczne podejmowanie istotnych decyzji wobec osoby, której dane dotyczą, **osoba** ta **ma prawo do tego, aby nie podlegać takiej decyzji**.

Gdy skutkiem profilowania jest automatyczne podejmowanie istotnych decyzji wobec osoby, której dane dotyczą, osoba ta ma prawo do tego, aby nie podlegać takiej decyzji.

Decyzje będą istotne, jeżeli wywoływać będą wobec tej osoby skutki prawne lub

w podobny sposób istotnie będą na nią wpływały.

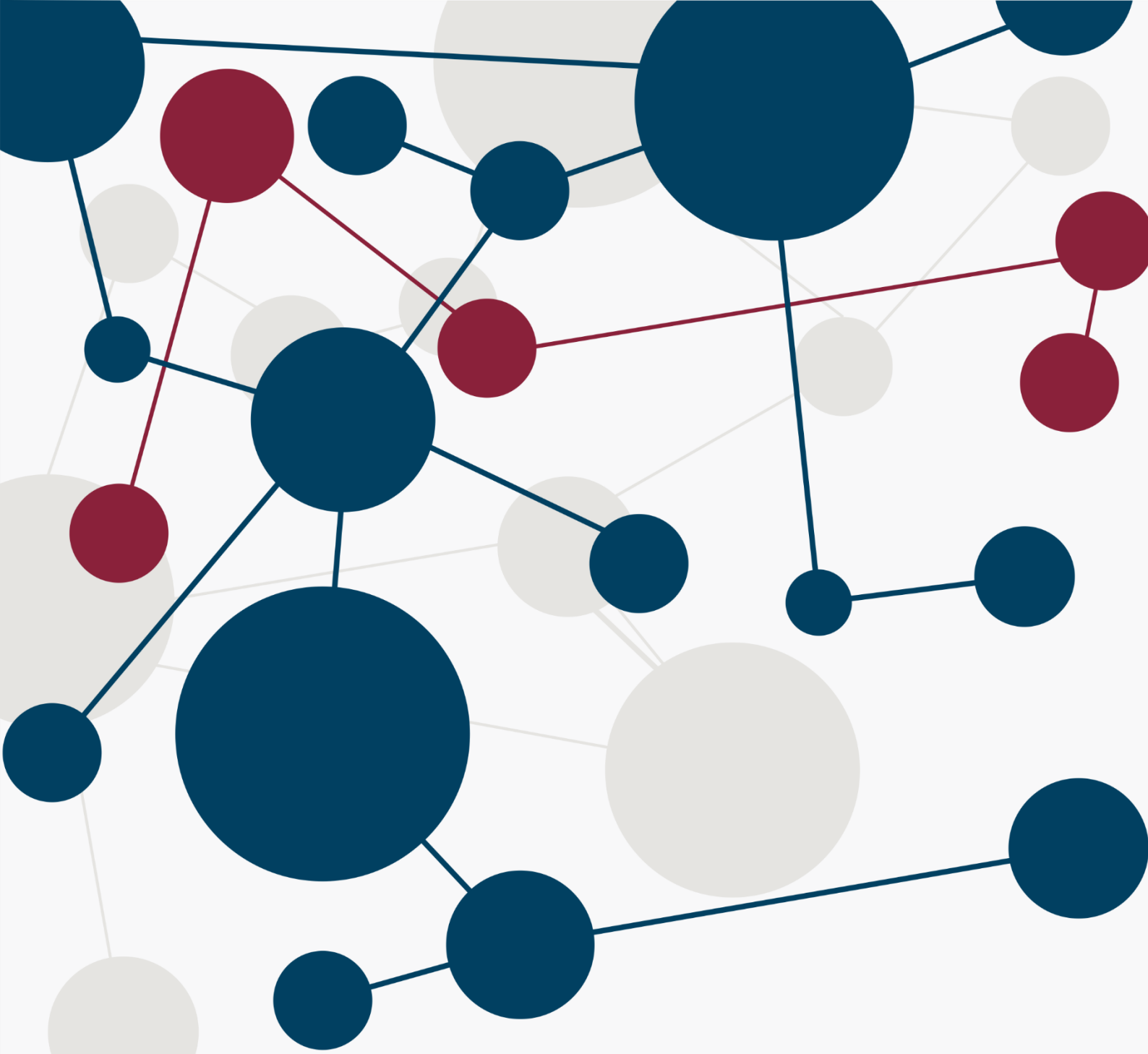
Prawo to nie ma zastosowania, gdy decyzja:

- jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą a administratorem;
- jest dozwolona prawem UE lub prawem państwa członkowskiego, któremu podlega administrator, ponadto wymagane jest, aby ta prawna podstawa przewidywała środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;
- jest oparta na zgodzie osoby zainteresowanej.

W pierwszym (umowa) i trzecim (zgoda) przypadku administrator **obowiązany jest zapewnić środki ochrony praw, wolności i interesów osoby, której dane dotyczą.** Minimalny sposób realizacji powyższych środków polega na zapewnieniu:

- interwencji ludzkiej ze strony administratora;
- zakwestionowaniu decyzji przez osobę, której dane dotyczą;
- wyrażenia własnego zdania.

Warto w tym miejscu nadmienić, że **Europejska Rada Ochrony Danych**, która zostanie utworzona z chwilą rozpoczęcia obowiązywania RODO, wyposażona jest w kompetencje do tego, **aby wydawać wytyczne, zalecenia i określać najlepsze praktyki** m.in. kryteriów i wymogów dotyczących decyzji opartych na profilowaniu.



RODO 2018

wprowadzenie do zmian

Rozdział VI

Rozdział VI. **Administracja danymi w RODO**

Niezależnie od obowiązków wymienionych do tej pory, Administrator **musi zapewnić odpowiednie środki techniczne i organizacyjne**, które zapewnią bezpieczeństwo danych, adekwatnie do ich charakteru, zakresu, kontekstu i celów przetwarzania. Przy ich opracowaniu i wdrażaniu administrator musi mieć na uwadze **ryzyko naruszenia praw oraz wolności osób fizycznych** oceniane z uwzględnieniem prawdopodobieństwa i wagi zagrożeń.

1. Obowiązki administratora

Niezwykle istotny jest fakt, że **administrator zobowiązany jest do wykazania wprowadzenia odpowiednich środków technicznych i organizacyjnych**, które służą do zabezpieczenia danych osobowych.

Oznacza to, że administrator zobowiązany jest dysponować stosowną dokumentacją w tym zakresie, celem przedstawienia organom nadzorczym dowodów na wypełnienie spoczywających na administratorze obowiązków.

> Administrator powinien stosować odpowiednią politykę ochrony danych.

W celu zapewnienia zgodnego z prawem przetwarzania danych administrator powinien stosować odpowiednią **politykę ochrony danych.**

Administrator **może także skorzystać z zatwierdzonych mechanizmów certyfikacji lub zatwierdzonych kodeksów postępowania** celem wykazania przestrzegania ciążących na nim obowiązków.

2. Współadministratorzy

Za **współadministratorów** RODO uważa co najmniej dwóch administratorów, **którzy wspólnie ustalają cele i sposoby przetwarzania.**

> Za współadministratorów RODO uważa co najmniej dwóch administratorów, którzy wspólnie ustalają cele i sposoby przetwarzania.

Przepisy nie regulują podstawowego zakresu odpowiedzialności współadministratorów, tj. nie wyznaczają, które obowiązki mają być przez którego z administratorów wykonywane – całość pozostawiona jest **wspólnym uzgodnieniom, które w przypadku podmiotów prywatnych powinny przybrać postać umowy.**

W uzgodnieniach tych należy określić **podział odpowiedzialności w związku z prawami** realizowanymi przez osoby, których dane dotyczą. Osoby udostępniające

lub chcące udostępnić własne dane, **mają prawo poznać zasadniczą treść uzgodnień między współadministratorami.**

Fakt wzajemnych uzgodnień nie może jednak wpływać negatywnie na prawa osób, których dane dotyczą. Osoby te **mogą realizować swoje prawa względem każdego z administratorów.**

3. Powierzenie przetwarzania

Szczególną uwagę należy poświęcić temu, jak RODO reguluje zagadnienia **powierzenia przetwarzania danych**. Ze względu na wagę ochrony danych osobowych administratorom nie pozostawiono nieograniczonej swobody. Wręcz przeciwnie – powierzenie takie podlega istotnym ograniczeniom.

Podmiotem przetwarzającym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Podmiotem przetwarzającym w rozumieniu przepisów jest **osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora**.

Przede wszystkim podmiot, któremu administrator powierza przetwarzanie **musi zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych**, dzięki którym możliwe będzie zapewnienie przetwarzania zgodnie z przepisami RODO.

Przykład

Przedsiębiorca XYZ S.A. jest administratorem zbioru danych, które to dane osobowe wykorzystuje w prowadzonej działalności gospodarczej polegającej na sprzedaży energii elektrycznej. W ramach reorganizacji prowadzonej działalności postanowiono o tym, że zadania biura obsługi klienta zostaną powierzone firmie zewnętrznej w ramach *outsourcingu*.

Do obsługi infolinii wytypowano trzy firmy. Jednakże okazało się, że w jednej z nich pracownicy w ogóle nie przechodzą szkoleń z zakresu ochrony danych, w drugiej natomiast – sprzęt komputerowy, na którym działać mają pracownicy, nie nadaje się do instalacji oprogramowania zabezpieczającego. Trzecia firma natomiast regularnie szkoli pracowników, posiada nowoczesny sprzęt komputerowy oraz odpowiednio zabezpiecza swoje zasoby.

W takiej sytuacji dopuszczalne będzie nawiązanie współpracy i powierzenie przetwarzania danych osobowych wyłącznie firmie trzeciej, gdyż tylko ona z powyższego grona daje rękojmię prawidłowego przetwarzania i jest wyposażona w adekwatne zabezpieczenia technologiczno-organizacyjne.

RODO dopuszcza również **zlecenie dalszego powierzenia przetwarzania danych osobowych przez podmiot przetwarzający.** Podmiot przetwarzający, który zleca dalsze przetwarzanie kolejnemu podmiotowi

obowiązany jest uzyskać pisemną zgodę administratora – szczegółową lub ogólną. W przypadku zgody ogólnej podmiot przetwarzający zobowiązany jest do informowania administratora każdorazowo o zamiarze przekazania przetwarzania dalej (na co administratorowi przysługuje sprzeciw) **oraz musi wybrać taki podmiot, który spełnia odpowiednie warunki** (dot. zapewnienia przetwarzania danych zgodnie z prawem).

Gwarancje można wykazać posługując się zatwierdzonym mechanizmem certyfikacji lub zatwierdzonym kodeksem postępowania.

Gwarancje (zarówno w przypadku powierzenia, jak i podpowierzenia) można wykazać posługując się **zatwierdzonym mechanizmem certyfikacji lub zatwierdzonym kodeksem postępowania.**

Powierzenie przetwarzania danych jest dopuszczalne na podstawie umowy lub innego instrumentu prawnego, który w naszej ocenie należy rozumieć jako akt prawa powszechnie obowiązującego. **Umowa o powierzenie przetwarzania danych musi być zawarta w formie pisemnej lub w formie elektronicznej**.

Konstrukcja umowy powierzenia przetwarzania powinna zawierać m.in. następujące zobowiązania nakładane na podmiot przetwarzający:

- przetwarzanie odbywa się wyłącznie na udokumentowane polecenie administratora;
- zobowiązanie do zachowania tajemnicy przez osoby, które będą upoważnione do przetwarzania danych;
- zobowiązanie do postępowania zgodnie z wymogami bezpieczeństwa przetwarzania określonymi w art. 32 RODO;
- w zależności od charakteru przetwarzania zobowiązanie do wspomagania w miarę możliwości, administratora w realizowaniu praw przysługujących osobom, których dane dotyczą;
- w zależności od charakteru przetwarzania zobowiązanie do wspomagania administratora w wywiązywaniu się z obowiązków związanych z wymogami bezpieczeństwa;
- po zakończeniu świadczenia usług związanych z przetwarzaniem, zobowiązanie do usunięcia wszelkich danych lub ich zwrócenia i usunięcia wszystkich ich kopii (chyba, że prawo Unii lub prawo państwa członkowskiego nakazuje dalsze przechowywanie);
- zobowiązanie do umożliwienia administratorowi przeprowadzania inspekcji i audytów;
- zobowiązanie do przekazywania administratorowi wszystkich informacji, które są niezbędne do wykazania spełnienia obowiązków przetwarzania danych.

Ponadto, na podmiocie przetwarzającym ciąży obowiązek informowania administratora o tym, że wydane polecenie **prowadzi do naruszenia przepisów o ochronie danych osobowych.**

4. Rejestrowanie czynności przetwarzania

Unijne regulacje nakładają na administratorów danych nowy obowiązek, polegający na **prowadzeniu rejestru czynności przetwarzania.** Drugim rodzajem rejestru przewidzianym przez RODO jest **rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora,** który prowadzony jest przez podmioty przetwarzające.

Unijne regulacje nakładają na administratorów danych nowy obowiązek – prowadzenie rejestru przetwarzania.

Do ich prowadzenia zobowiązane są podmioty zatrudniające 250 i więcej osób. Zasadą jest, że podmioty mniejsze nie są zobowiązane do prowadzenia powyższych rejestrów oprócz takich sytuacji, gdy:

- może powstawać ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
- przetwarzanie nie ma charakteru sporadycznego;
- rejestr obejmuje dane wrażliwe (w tym dotyczące wyroków skazujących i naruszeń prawa).

W zasadzie **każdy administrator zatrudniający pracowników przetwarza ich dane osobowe częściej niż sporadycznie**. W konsekwencji, w zależności od przyjętej interpretacji przepisów, wyjątek związany z nietworzeniem rejestrów może okazać się iluzoryczny.

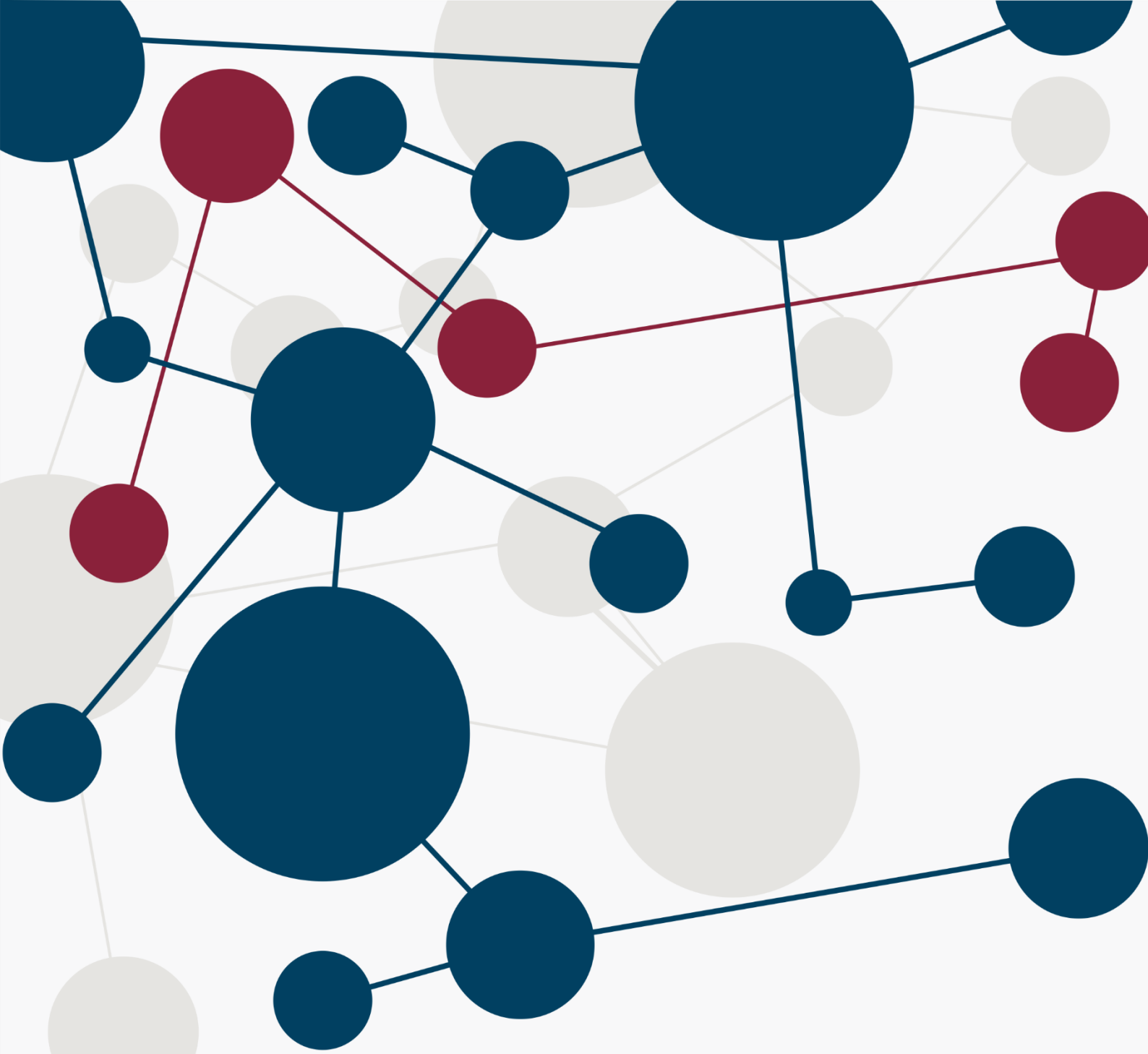
Powyższe rejestry powinny być prowadzone **w formie pisemnej, w tym elektronicznej.** Takie sformułowanie oznacza, że prowadzenie rejestru w formie elektronicznej będzie równoważne prowadzeniu go w formie pisemnej i będzie wypełnieniem obowiązku.

Niedopełnienie obowiązku prowadzenia rejestru może skutkować nałożeniem kary w wysokości do 10 000 000 euro lub 2% rocznego światowego obrotu.

Niedopełnienie obowiązku prowadzenia rejestru **może skutkować nałożeniem przez organ nadzorujący kary pieniężnej w wysokości do 10 000 000 euro lub 2% rocznego światowego obrotu** (w przypadku przedsiębiorstw). Nałożona zostanie kara, która będzie kwotowo **wyższa** spośród wyliczonych w tych granicach. Podmioty, które prowadzą rejestr, obowiązane są udostępnić go na żądanie organu nadzorczego. Rejestry te mają określoną prawem przewidzianą zawartość.

Tabela 1 Rejestry wymagane przepisami RODO

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH (ADMINISTRATOR)	REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DOKONYWANYCH W IMIENIU ADMINISTRATORA (PODMIOT PRZETWARZAJĄCY)
Imię i nazwisko bądź nazwa administratora lub współadministratorów	Imię i nazwisko bądź nazwa podmiotu przetwarzającego
Dane kontaktowe administratora lub współadministratorów	Dane kontaktowe podmiotu przetwarzającego
Jeżeli ustanowiono – imię i nazwisko oraz dane kontaktowe inspektora ochrony danych	Jeżeli ustanowiono – imię i nazwisko oraz dane kontaktowe inspektora ochrony danych
Cele przetwarzania	Kategorie przetwarzań dokonywanych w imieniu każdego z administratorów
Gdy ma to zastosowanie – informacje o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej; nazwa tego państwa lub organizacji; gdy jest to wymagane – dokumentacja odpowiednich zabezpieczeń	Gdy ma to zastosowanie – informacje o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej; nazwa tego państwa lub organizacji; gdy jest to wymagane – dokumentacja odpowiednich zabezpieczeń
Jeżeli jest to możliwe, ogólny opis techniczno-organizacyjnych środków bezpieczeństwa	Jeżeli jest to możliwe, ogólny opis techniczno-organizacyjnych środków bezpieczeństwa
Kategorie odbiorców, którym udostępnia się dane	Dane każdego administratora, w imieniu którego przetwarzane są dane
Opis kategorii osób, których dane dotyczą	
Opis kategorii danych osobowych	
Planowany termin usunięcia poszczególnych kategorii danych osobowych (jeżeli jest to możliwe do określenia)	



RODO 2018

wprowadzenie do zmian

Rozdział VII

Rozdział VII. **Bezpieczeństwo danych**

Aby zapewnić skuteczną ochronę danych osobowych, RODO określa wytyczne w zakresie zapewnienia bezpiecznego przetwarzania danych osobowych. Wytyczne te nie są ustalone „na sztywno". Każdorazowo administrator i podmiot przetwarzający musi ustalić optymalny sposób ochrony danych.

1. Minimalny standard ochrony w RODO

Opracowując więc **środki bezpieczeństwa** (zarówno o charakterze organizacyjnym, jak i te o charakterze technicznym), należy brać pod uwagę **stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.**

W RODO zawarte zostały pewne **przykłady odpowiednich środków technicznych i organizacyjnych**:

- pseudonimizację i szyfrowanie danych osobowych;
- zapewnienie ciągłej poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- umożliwienie szybkiego przywrócenia dostępności danych osobowych oraz umożliwienie dostępu do nich w przypadkach wystąpienia incydentów fizycznych lub technicznych, przykładowo należy skonstruować system informatyczny w taki sposób, aby można było skorzystać z kopii zapasowej danych, aby w optymalnym czasie przywrócić pełną sprawność systemu;
- regularne testowanie i ocenianie wdrożonego systemu bezpieczeństwa (środków technicznych oraz organizacyjnych).

Oczywiście nie są to jedyne środki, do podjęcia których zobowiązani są administratorzy, czy podmioty przetwarzające. Co więcej **może się zdarzyć, że przedstawione powyżej przykłady zostaną ocenione za niewystarczające** w przypadku danego administratora danych lub podmiotu przetwarzającego z uwagi na wykonywane przez niego działania w zakresie przetwarzania danych osobowych.

Przykład

Przedsiębiorca jest administratorem zbioru danych, zawartych w bazie danych na jego serwerze. Gromadzone są tam dane klientów: imiona, nazwiska, adresy i numery kart płatniczych oraz banki je wydające. W takiej sytuacji, osoba niepożądana, która uzyskałaby dostęp do serwera miałaby również dostęp do pełnego kompletu danych osobowych.

Aby zwiększyć bezpieczeństwo danych podjęto decyzję o zastosowaniu pseudonimizacji. W tym celu wykupiono osobny serwer, na którym stworzono nową bazę danych, do której przeniesiono imiona i część adresu (ulica i kod pocztowy) oraz niektóre cyfry numerów kart płatniczych każdego klienta. W obydwu bazach nadano

rekordom unikalne numery. W ten sposób więc, kojarząc numer z bazy zawierającej imiona i nazwiska z numerem, znajdującym się w bazie z resztą danych, uzyskujemy dopiero komplet informacji.

W takiej sytuacji, jeżeli osoba niepowołana uzyskałaby dostęp do jednej tylko bazy, ujrzałaby samoistnie niewiele warte dane – wszak znając samo tylko nazwisko i niektóre cyfry z numeru karty płatniczej danej osoby, osoba nieupoważniona będzie miała utrudnioną możliwość wykorzystania tych informacji dla swoich korzyści. Identyfikacja osoby, której dane dotyczą wymagałaby najpewniej realizacji kolejnych działań pozwalających uzyskać o danej osobie więcej informacji.

W dzisiejszych czasach przetwarzanie danych odbywa się najczęściej z wykorzystaniem komputerowych baz danych. **Opracowywanie i wdrażanie odpowiednich systemów bezpieczeństwa wymagać będzie ścisłej współpracy między informatykami oraz prawnikami wyspecjalizowanymi w zakresie ochrony danych osobowych.**

2. Ocena ryzyka związanego z przetwarzaniem danych

RODO wskazuje również kryteria, na podstawie których należy dokonywać oceny stosowanych środków bezpieczeństwa.

Kryterium, na które szczególną uwagę zwraca RODO, to **poziom ryzyka** występującego **przy przetwarzaniu danych.**

Przy **ocenie tegoż ryzyka** należy brać pod uwagę konsekwencje przypadkowego lub niezgodnego z prawem:

- zniszczenia;
- utraty;
- modyfikacji;
- ujawnienia;
- dostępu do danych.

Ryzyko to należy oceniać na każdym etapie przetwarzania danych, w tym ich przesyłania czy przechowywania.

Administrator (podmiot przetwarzający), w ramach zapewnienia środków bezpieczeństwa, obowiązany jest zapewnić, aby **każda osoba fizyczna działająca z jego upoważnienia, która ma dostęp do danych, przetwarzała je wyłącznie na polecenie administratora.**

3. Zgłoszenia i zawiadomienia o naruszeniu ochrony danych osobowych

RODO nakłada na administratorów obowiązek odpowiednich zgłoszeń i zawiadomień w sytuacjach, **gdy dojdzie do naruszenia przepisów** o ochronie danych osobowych. **Zgłoszenia** dotyczą informowania **organu nadzorczego** o zaistniałym naruszeniu**. Zawiadomienia** dotyczą zaś informowania **osób, których dane dotyczą** o zaistniałym naruszeniu.

3.1. Zgłoszenie naruszenia organowi nadzorczemu

Obowiązek zgłoszenia naruszenia organowi nadzorczemu (w odniesieniu do administratora) powstaje z momentem stwierdzenia naruszenia. Zgłoszenia takiego należy dokonać **niezwłocznie,** nie później jednak niż **w ciągu 72 godzin.** Jeżeli do zgłoszenia dojdzie później, to należy dołączyć stosowne wyjaśnienia tłumaczące przyczyny opóźnienia.

W przypadku, gdy naruszenie stwierdzi podmiot przetwarzający, to musi on bez zbędnej zwłoki poinformować administratora o zaistniałym naruszeniu.

Przepisy przewidują minimalną treść zgłoszenia. **Zgłoszenie takie powinno zawierać:**

- opis charakteru naruszenia ochrony danych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dotyczy naruszenie oraz kategorie i przybliżoną liczę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe inspektora danych osobowych lub wskazanie innego punktu kontaktowego; oznaczenia te zamieszcza się w celu dalszego kontaktu;
- opis możliwych konsekwencji naruszenia, ten element zgłoszenia należy uznać za bardzo istotny, jednak wymagający od administratora istotnego nakładu pracy;
- opis zastosowanych bądź proponowanych środków przedsięwziętych/do przedsięwzięcia w celu zaradzenia naruszeniu ochrony danych, jeżeli jest to w danym przypadku możliwe; należy również uwzględnić środki mające na celu minimalizację negatywnych skutków naruszenia.

W przypadku naruszeń na większą skalę administrator może nie być w stanie zgłosić organowi nadzorczemu wszystkich wymienionych powyżej informacji w przeciągu 72 godzin. Powyższe zostało uwzględnione przez prawodawcę unijnego, który **zezwala na przekazywanie kolejnych informacji (partiami) w czasie późniejszym, jednak bez zbędnej zwłoki**. W takiej sytuacji mimo wszystko zgłoszenia należy dokonać w przeciągu 72 godzin.

Ponadto, administrator obowiązany jest do **prowadzenia dokumentacji naruszeń.** Musi ona zawierać informacje o tych naruszeniach, w tym w szczególności **okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze.** Musi ona być skonstruowana w taki sposób, aby organ nadzorczy miał możliwość weryfikacji przestrzegania obowiązku zgłaszania naruszeń.

Obowiązek zgłaszania jest zasadą.

Obowiązek zgłaszania jest zasadą. Zwolnić można się z niego jedynie wtedy, gdy mało prawdopodobnym jest, aby naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych. Z konstrukcji przepisu („chyba, że jest mało prawdopodobne […]", art. 33 ust. 1 zdanie 1 RODO) wynika jednak, że domniemywa się, iż takie ryzyko istnieje. W konsekwencji to na administratorze będzie ciążył obowiązek wykazania, że tak nie jest.

3.2. Zawiadomienie osób, które udostępniły dane

W odniesieniu do **zawiadamiania osób, których dane dotyczą,** obowiązek zawiadomienia powstaje tylko wtedy, gdy naruszenie może powodować **wysokie ryzyko naruszenia praw lub wolności osoby**. W takiej sytuacji **administrator zawiadamia osobę, że do naruszenia doszło.** Zawiadomienia należy dokonać bez

zbędnej zwłoki. Przepisy nie zakreślają jednak dokładnego terminu dokonania zawiadomienia, jak to ma miejsce w przypadku zgłoszenia naruszenia organowi nadzorczemu. Niemniej jednak należy wychodzić z założenia, że im szybciej zostanie to dokonane, tym lepiej.

Administrator, dokonując zawiadomienia, musi **jasnym i prostym językiem** przedstawić co najmniej:

- opis charakteru naruszenia;
- imię i nazwisko oraz dane kontaktowe inspektora danych lub jakiegokolwiek innego punktu kontaktowego w celu uzyskiwania dalszych informacji;
- opis możliwych konsekwencji naruszenia;
- opis środków zastosowanych lub proponowanych do zaradzenia naruszeniu i minimalizacji ewentualnych szkód.

Administrator nie jest obowiązany do dokonania zawiadomienia, gdy:

- administrator wdrożył odpowiednie środki (zarówno techniczne, jak i organizacyjne) oraz środki te zostały zastosowane w stosunku do danych osób, których dotyczy naruszenie (innymi słowy, wdrożenie odpowiednich środków może ograniczyć wysokie ryzyko naruszenia praw lub wolności osób fizycznych);
- administrator zastosował środki, które eliminują prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób, których dotyczą dane dotknięte naruszeniem;
- zawiadamianie wymagałoby niewspółmiernie dużego wysiłku.

W trzecim przypadku nie oznacza to jednak, że administrator może zaniechać informowania.

W takiej sytuacji musi on jednak wydać **publiczny komunikat** (lub zastosować podobny do tego środek), **który zapewni skuteczne poinformowanie osób, których dane dotyczą**. Oczywiście poinformowanie osób fizycznych poprzez publiczny komunikat zawsze rodzi ryzyko, że nie zostanie on odebrany przez wszystkich potencjalnych adresatów. To samo jednak można uznać w przypadku podjęcia próby indywidualnego poinformowania osób, których dane dotyczą.

4. DPIA – nowa procedura oceny w RODO

Data Protection Impact Assesment, czyli ocena skutków dla ochrony danych, zwana również DPIA jest procedurą, która ma na celu odpowiednie przygotowanie administratora do przetwarzania danych w sposób zgodny z RODO.

Data Protection Impact Assesment, czyli ocena skutków dla ochrony danych.

Nie dotyczy ona przetwarzania danych przez wszystkich administratorów. DPIA przeprowadza się w przedsięwzięciach o podwyższonym ryzyku dla ochrony danych, o czym mowa poniżej.

Służy ono do zapewnienia przetwarzania zgodnego z prawem oraz do celów rozliczania się z organem nadzorczym (zważywszy na fakt, że na administratorze ciąży obowiązek wykazywania zgodności przetwarzania z prawem).

DPIA jest wprowadzane przez art. 35 RODO, w którym to prawodawca unijny zawarł ogólne ramy tej procedury. Jest ona również immanentnie związana z konsultacjami z organem nadzorczym (art. 36 RODO). Regulacje te są, jak już wspomniano, dość ogólne i **Grupa Robocza art. 29 opracowała wytyczne**[3], w których doprecyzowuje przepisy RODO.

5. DPIA – kiedy przeprowadzić?

Procedurę należy przeprowadzić **przed rozpoczęciem przetwarzania.** DPIA można więc powiązać z realizacją zasady *privacy by design.*

> Procedurę należy przeprowadzić przed rozpoczęciem przetwarzania.

RODO określa, że DPIA przeprowadza się w odniesieniu do **operacji przetwarzania danych,** jednakże tylko takich, które **z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw i wolności osoby fizycznej.** W szczególności przeprowadzenie oceny skutków dla ochrony danych jest wymagane w następujących przypadkach:

- systematycznej i kompleksowej oceny czynników odnoszących się do osoby fizycznej; ocena czynników winna opierać się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, gdy jest to podstawą decyzji wywołujących skutki prawne wobec osoby lub w podobny sposób znacząco na nią wpływającej;
- przetwarzania na dużą skalę danych wrażliwych; będzie się to np. odnosić do placówek opieki zdrowotnej;
- systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Dla podobnych operacji przetwarzania danych wiążących się z podobnym ryzykiem można przeprowadzić pojedynczą ocenę skutków**.**

Zgodnie z wytycznymi Grupy Roboczej art. 29 dopuszczalna jest również sytuacja taka, że np. producent oprogramowania, które wykorzystywane jest do przetwarzania danych, samodzielnie przeprowadzi taką analizę, którą dostarczy administratorowi a administrator ten będzie mógł się później nią posługiwać.

Przykładowymi sytuacjami, gdy przetwarzanie „może z dużym prawdopodobieństwem powodować wysokie ryzyko" mogą również być monitorowanie imprez masowych – ze względu na to, że osoba może nie być świadoma, że jest nagrywana oraz nie wie, w jaki sposób te dane zostaną w przyszłości wykorzystane.

Wyjaśnić z pewnością należy pojęcie **dużej skali przetwarzania** w odniesieniu do **danych wrażliwych.** Grupa Robocza art. 29 w wytycznych wskazuje, że należy brać pod uwagę czynniki takie, jak **liczba osób, których dane dotyczą, zakres przetwarzanych danych osobowych, okres, przez**

[3] Oryginalna wersja wytycznych znajduje się pod adresem: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (dostęp na dzień 5 lipca 2017 r.).

jaki dane są przetwarzane, zakres geograficzny przetwarzania danych.

Grupa Robocza art. 29 wymienia następujące kryteria, które należy brać pod uwagę oceniając konieczność przeprowadzania DPIA**:**

- czy dochodzi do oceny, w tym profilowania, osoby fizycznej na podstawie danych osobowych;
- czy dochodzi do zautomatyzowanego podejmowania decyzji wywołujących skutki prawne lub podobne istotne skutki wobec osoby;
- czy sytuacja polega na systematycznym monitorowaniu miejsc;
- czy przetwarzane są dane wrażliwe;
- czy przetwarzanie odbywa się na dużą skalę;
- czy porównano lub połączono zestawy danych w sposób wykraczający poza racjonalne oczekiwania osoby, której dane dotyczą;
- czy dane dotyczą osób wymagających szczególnej opieki, np. dzieci, osoby psychicznie chore;
- czy dochodzi do innowacyjnego wykorzystania lub zastosowania rozwiązań technologicznych;
- czy dane osobowe są przekazywane poza Unię;
- czy przetwarzanie samo w sobie nie uniemożliwia osobom, których dane dotyczą wykonywanie prawa lub korzystanie z usługi lub umowy (chodzi m. in. o takie operacje przetwarzania, których wynik mógłby uniemożliwić skorzystanie z jakiejś usługi, a przetwarzanie odbywałoby się bez czynnika ludzkiego).

Zgodnie z zaleceniami Grupy Roboczej art. 29 **spełnienie dwóch z powyższych kryteriów** stanowi już wystarczającą wskazówkę, że prawdopodobieństwo wystąpienia wysokiego ryzyka istnieje i **przeprowadzenie DPIA jest zalecane.**

Nie można tego jednak uważać za wyznacznik, od którego nie ma odstępstw. Będą istniały takie sytuacje, gdzie **nawet spełnienie jednego z wyżej wskazanych warunków będzie kwalifikowało do przeprowadzenia DPIA**.

> Będą istniały sytuacje, gdzie nawet spełnienie jednego z warunków będzie kwalifikowało do przeprowadzenia DPIA.

Pomimo tego, że DPIA jest elementem RODO, które w życie dopiero wejdzie, to jednak Grupa Robocza art. 29 wyraźnie zaleca przeprowadzenie DPIA względem operacji przetwarzania, które rozpoczęły się przed wejściem w życie przepisów, tj. 25 maja 2018 r. Wskazuje się również, że w przypadku operacji przetwarzania rozpoczętych wcześniej, w których jednak zajdą istotne zmiany po wejściu w życiu RODO, zmiana może być na tyle istotna, że przeprowadzenie DPIA będzie wymagane. W odniesieniu do tego stwierdzić jednak należy, że każdy przypadek powinien podlegać indywidualnej konsultacji z prawnikiem wykwalifikowanym w zakresie ochrony danych osobowych, aby zapewnić jak najtrafniejszą ocenę.

Jako dobrą praktykę wskazuje się **przeprowadzanie DPIA co najmniej raz na 3 lata,** co nie wyklucza jednak ciągłego

monitorowania czynności przetwarzania tak, aby zawsze zapewnić zgodność z prawem.

6. DPIA – zakres i sposób przeprowadzania

W przedmiocie przeprowadzania oraz zakresu procedury DPIA, RODO nie przedstawia zbyt wielu wskazówek. Określa jedynie **minimalny zakres**, który DPIA musi spełniać.

Tak więc, **poprawnie przeprowadzone DPIA musi zawierać co najmniej**:

- usystematyzowany opis planowanych operacji przetwarzania i celów przetwarzania;
- jeżeli występują – prawnie uzasadnione interesy, które administrator realizuje;
- ocenę proporcjonalności i niezbędności operacji przetwarzania w stosunku do celów;
- ocenę, czy występuje duże prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą;
- opis planowanych środków, przedsięwziętych w celu zaradzenia ryzyku, wliczając w to środki i mechanizmy bezpieczeństwa.

Opracowując opis środków, należy uwzględnić trzy kwestie. Po pierwsze, **zastosowane środki muszą zapewnić ochronę danych.** Po drugie, opis środków musi być również skonstruowany w taki sposób, aby administrator **był w stanie wykazać przestrzeganie przepisów RODO.**

Po trzecie zaś planowane środki muszą uwzględniać **prawa i prawnie uzasadnione interesy osób, których dane dotyczą.** W ramach DPIA należy więc uwzględnić jej **funkcję dokumentacyjną i rozliczeniową**.

Mając na uwadze wytyczne GR art. 29, schemat przeprowadzania DPIA można przedstawić za pomocą wykresu (patrz Rysunek 1 poniżej).

Rysunek 1: Wykres DPIA na podstawie wytycznych GR art. 29

W ocenie Autorów opis środków zgodności z RODO powinien zawierać się w opisie środków przewidzianych do redukcji ryzyka lub też stanowić samodzielny element, który należy przeprowadzić po ocenie ryzyka naruszenia praw i wolności osób, których dane dotyczą.

Nie można jednak zapomnieć o tym, że przetwarzanie danych jest sytuacją dynamiczną. Zmieniają się metody, cele, środki bezpieczeństwa. Realizując etap **monitorowania i reagowania**, należy brać pod uwagę właśnie czynnik zmienności. Jeżeli więc operacja przetwarzania, dla której DPIA zostało przeprowadzone zmieni się znacznie, to **koniecznym będzie przeprowadzenie nowego DPIA.**

7. Konsultacje z organem nadzorczym

RODO przewiduje obowiązek przeprowadzenia przez administratora konsultacji z organem nadzorczym, jeżeli taka potrzeba wyniknie z przeprowadzonej DPIA.

RODO przewiduje obowiązek przeprowadzenia przez administratora konsultacji z organem nadzorczym.

Zgodnie z art. 36 ust. 1 RODO, jeżeli DPIA wskaże, że przetwarzanie danych powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania należy skonsultować to przetwarzanie z organem nadzorczym.

Uwzględniając powyższe postanowienie, należy w zasadzie zawsze konsultować przetwarzanie danych z organem nadzorczym, jeżeli administrator uzna, że po przeprowadzonym DPIA istnieje wysokie ryzyko dla danych w przypadku braku zabezpieczeń. Rozwiązanie takie może być jednak zbyt daleko idące. Zwracamy bowiem uwagę na motyw 94 RODO. Zgodnie z jego treścią uprzednia konsultacja jest niezbędna jeżeli:

- niezastosowanie środków bezpieczeństwa powodować będzie występowanie wysokiego ryzyka naruszenia praw;
- i jednocześnie administrator wyraża opinię, że nie jest w stanie zminimalizować ryzyka z wykorzystaniem środków, których wprowadzenie jest rozsądne z punktu widzenia technologicznego i kosztów wdrożenia.

Kwestia ta nie jest jednoznaczna. Dla bezpieczeństwa sugerowalibyśmy konsultować z organem przypadki odpowiadające wyłącznie pierwszemu z wymienionych powyżej punktów, jednak w praktyce takie podejście będzie też nadmiernym formalizmem.

Konsultacje z organem inicjowane są wnioskiem administratora o ich przeprowadzenie.

Konsultacje z organem inicjowane są **wnioskiem administratora o ich przeprowadzenie.** Zgodnie z RODO administrator zobowiązany jest we wniosku o przeprowadzenie konsultacji:

- przedstawić organowi (jeżeli ma to zastosowanie) zakresy obowiązków odpowiednio ciążących na administratorze, współadministratorze i podmiotach przetwarzających;
- przedstawić cele oraz sposoby zamierzonego przetwarzania;
- przedstawić środki i zabezpieczenia;
- podać dane kontaktowe inspektora ochrony danych (jeżeli jest ustanowiony);
- przedstawić wynik DPIA przeprowadzonego do tej pory;
- udostępnić każdą inną informację, której zażąda organ.

Ponadto, samo prawo państwa członkowskiego może wymagać, aby administrator zwrócił się z wnioskiem o konsultację niezależnie od wyżej opisanych przesłanek i uzyskał jego uprzednią zgodę na przetwarzanie danych do celów wykonania zadania realizowanego przez administratora w interesie publicznym.

8. Inspektor ochrony danych

RODO likwiduje znanego z polskiej uodo ABI (administratora bezpieczeństwa informacji) i zastępuje tzw. inspektorem ochrony danych.

Zgodnie z obowiązującymi przepisami **ustanowienie administratora bezpieczeństwa informacji jest fakultatywne** (art. 36 uodo), niezależnie od okoliczności. RODO przewiduje w tym zakresie zmianę, gdyż unijne przepisy przewidują okoliczności, w których powołanie inspektora ochrony danych jest obowiązkowe.

Ta zmiana będzie dotyczyć następujących kategorii przypadków:

- gdy przetwarzanie dokonywane jest przez organ lub podmiot publiczny (z wyłączeniem sądów w zakresie sprawowanego przez nie wymiaru sprawiedliwości);
- gdy działalność administratora polega na takich operacjach przetwarzania, które ze względu na swój cel, charakter lub zakres wymagają regularnego i systematycznego monitorowania osób na dużą skalę;
- gdy główna działalność administratora polega na przetwarzaniu na dużą skalę danych wrażliwych,
- jeżeli wymaga tego prawo Unii Europejskiej lub prawo państwa członkowskiego.

W każdym z tych przypadków ustanowienie inspektora ochrony danych (dalej „**inspektora**") **będzie obowiązkiem administratora.**

Przepisy pozwalają na ustanowienie jednego, wspólnego inspektora dla grupy przedsiębiorców, jeżeli każda jednostka organizacyjna będzie mogła uzyskać łatwy z nim kontakt.

Warto zauważyć, że przepisy pozwalają na ustanowienie jednego, wspólnego inspektora dla grupy przedsiębiorców, **jeżeli każda jednostka organizacyjna będzie mogła uzyskać łatwy z nim kontakt.**

Inspektorem nie może zostać dowolna osoba. Podobnie jak uodo, RODO przewiduje, że inspektor musi posiadać **odpowiednie kwalifikacje zawodowe, a w szczególności fachową wiedzę na**

temat ochrony danych osobowych oraz mieć umiejętności, które pozwolą mu wykonywać swoje zadania. Administrator danych ma obowiązek **włączać inspektora we wszystkie sprawy dotyczące ochrony danych w swojej organizacji.** Ponadto, musi mu zapewnić wsparcie i zasoby do wykonywania zadań oraz zasoby niezbędne do utrzymania fachowej wiedzy (przez co należy chociażby rozumieć zapewnianie uczestnictwa i sfinansowanie inspektorowi udziału w szkoleniach). Inspektorowi **należy zapewnić niezależność w wykonywaniu zadań.**

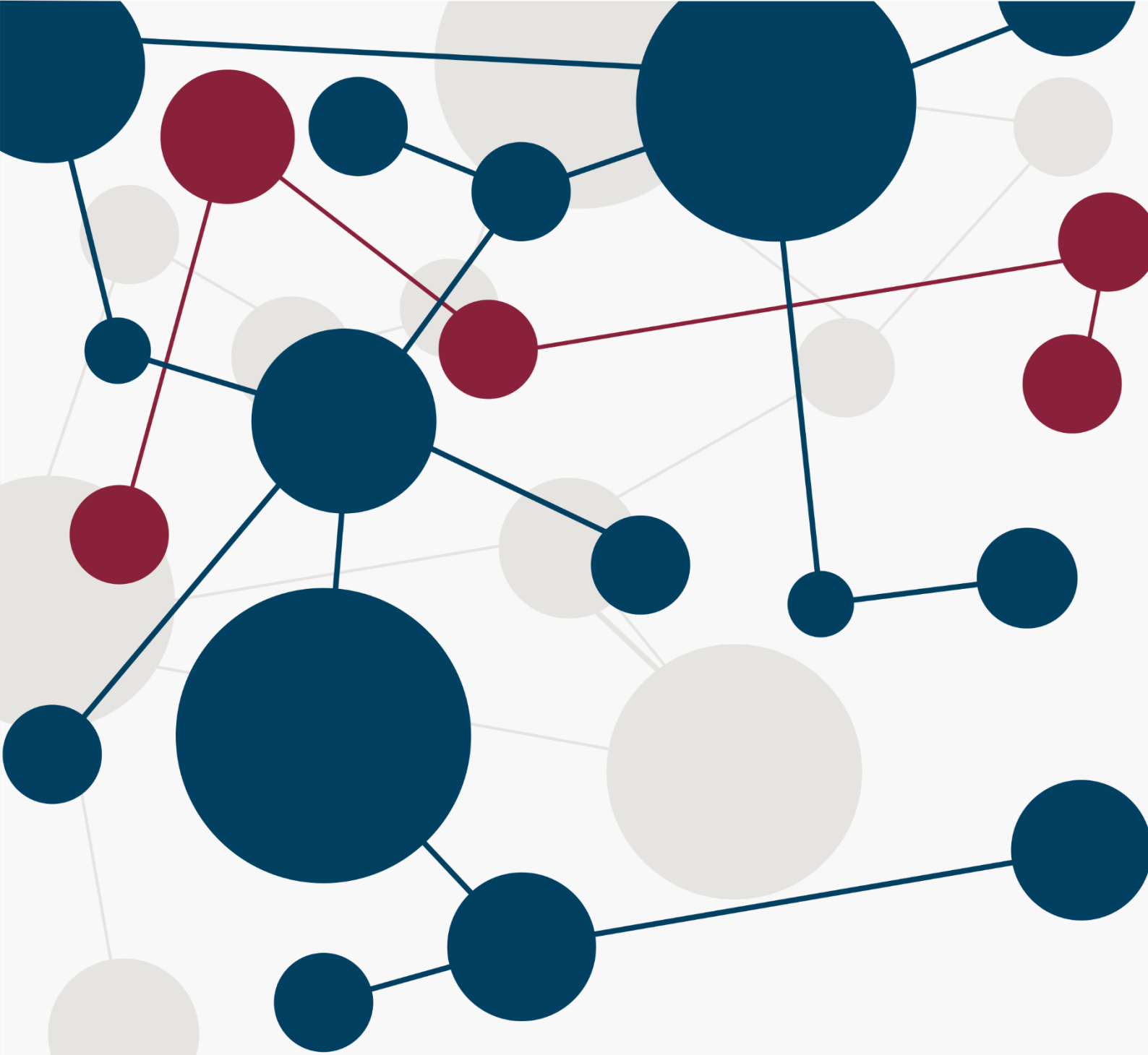
Inspektorowi należy zapewnić niezależność w wykonywaniu zadań.

Administrator nie ma prawa wydawać instrukcji inspektorowi w zakresie, w jakim wykonuje swoje zadania. Nie może on być również karany ani odwoływany za wypełnianie swoich zadań (przyjąć należy, że chodzi o kary za prawidłowe wykonywanie zadań, które czasami może być sprzeczne z partykularnym interesem administratora).

W zakresie jego zadań znajduje się:

- udzielanie administratorowi, podmiotowi przetwarzającemu oraz ich pracownikom informacji o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych;
- doradztwo w zakresie ochrony danych;
- udzielanie zaleceń, co do DPIA oraz monitorowanie wykonywania DPIA;
- monitorowanie przestrzegania prawa w zakresie ochrony danych oraz przyjętych polityk administratora lub podmiotu przetwarzającego;
- działania zwiększające świadomość w zakresie ochrony danych, prowadzenie szkoleń i audytów;
- współpraca z organem nadzorczym oraz pełnienie roli punktu kontaktowego.

Inspektor zobowiązany jest do zachowania tajemnicy co do wykonywanych zadań. Warto zauważyć, że **inspektor może wykonywać inne zadania i obowiązki, o ile zadania te nie będą powodowały konfliktu interesów**.



RODO 2018

wprowadzenie do zmian

Rozdział VIII

Rozdział VIII. **Przekazywanie danych osobowych do państw trzecich**

Przekazywanie danych osobowych do państw trzecich (które nie są członkami Unii Europejskiej) i organizacji międzynarodowych wymaga spełnienia odpowiednich wymogów, których podstawowym założeniem jest zapewnienie, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w RODO. Innymi słowy przekazując dane osobowe do państw trzecich, należy – co do zasady – podjąć takie działania, aby podmiot, który otrzyma te dane, zabezpieczył je w sposób odpowiadający RODO.

Problematyka przekazywania danych osobowych do państw trzecich wykracza jednak poza ramy niniejszej publikacji z uwagi na swoją złożoność. W tym miejscu wskażemy tylko na pewne ogólne rozwiązania w tym zakresie.

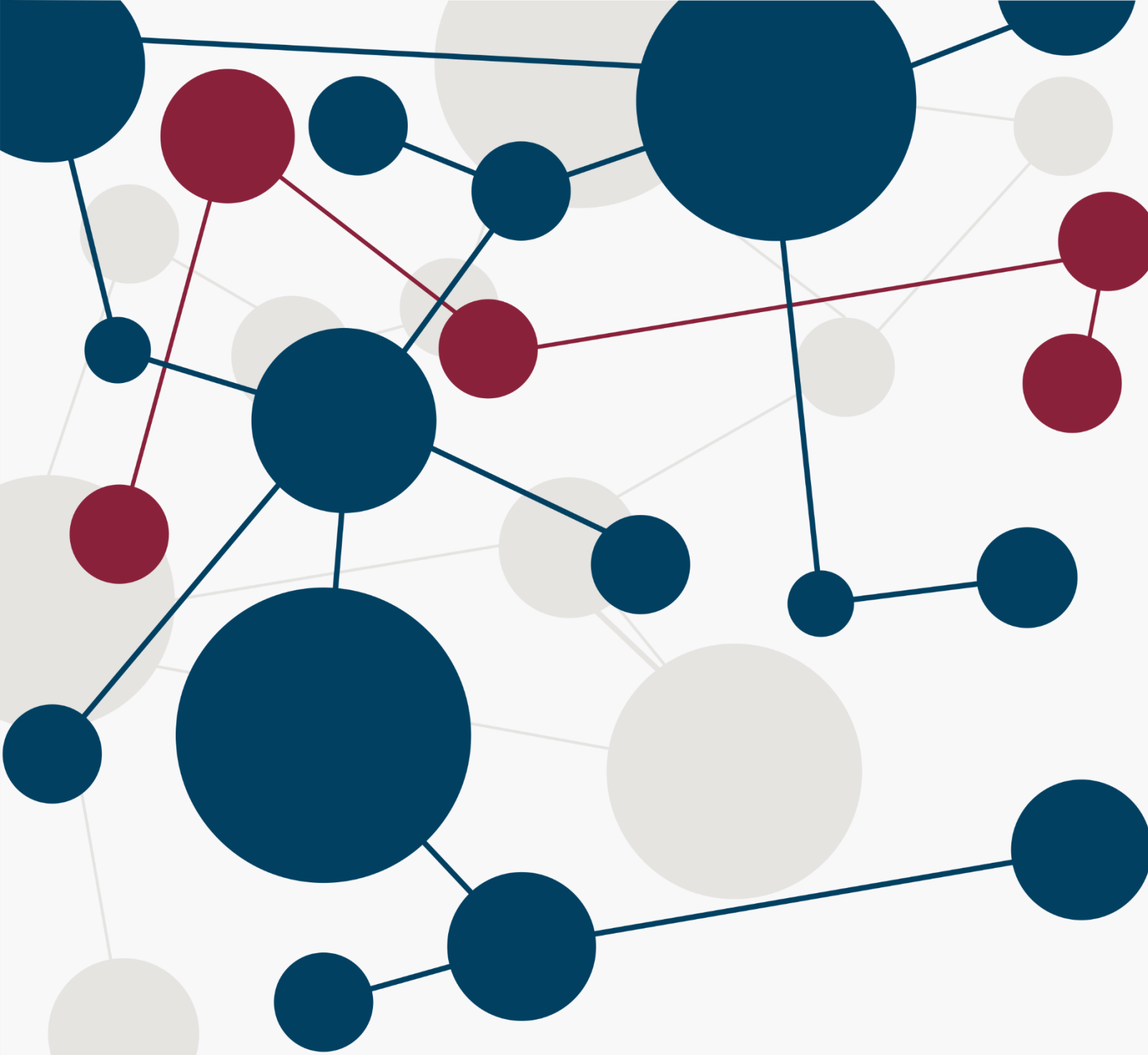
Przekazywanie danych osobowych do Państwa trzeciego może nastąpić m.in. w następujących przypadkach:

- Komisja Europejska stwierdzi, że dane państwo lub jego obszar zapewniają odpowiedni stopień ochrony;
- jeżeli zostaną zapewnione odpowiednie zabezpieczenia np. na podstawie stosunku umownego bazującego na tzw. standardowych klauzulach ochrony danych przyjętych przez Komisję Europejską;
- na podstawie zatwierdzonych przez organ nadzorczy wiążących reguł korporacyjnych;
- na podstawie stosunku umownego bazującego na tzw. standardowych klauzulach ochrony danych przyjętych przez Komisję Europejską;
- na podstawie zatwierdzonych przez organ nadzorczy wiążących reguł korporacyjnych;
- na podstawie decyzji zezwalającej wydanej przez organ nadzorczy.

Można jednak przekazać dane osobowe do państwa trzeciego nawet, gdy nie są spełnione odpowiednie wymagania m.in. w następujących przypadkach:

- osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, wyraźnie wyrazi na to zgodę;
- przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą a administratorem;
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą między administratorem a innym podmiotem.

W tym miejscu zaznaczamy, że powierzenie przetwarzania danych osobowych jest również przekazaniem danych do państwa trzeciego.



RODO 2018

wprowadzenie do zmian

Rozdział IX

Rozdział IX. **Odpowiedzialność za naruszenie zasad przetwarzania**

Nowym narzędziem w ręku krajowych organów ochrony danych osobowych będzie wymierzanie administracyjnych kar pieniężnych. Dotychczas w kompetencjach GIODO nie leżało karanie naruszeń, lecz dbanie o zgodność przetwarzania z prawem przez ewentualne korygowanie naruszeń.

RODO wyposaża organ nadzorczy w kompetencje do stosowania działań o charakterze represyjnym.

RODO wyposaża organ nadzorczy w kompetencje do stosowania działań o charakterze represyjnym. W motywach rozporządzenia organy unijne wskazują, że ma być to narzędzie do skutecznego egzekwowania naruszeń.

Wysokość kary jest niebagatelna, gdyż może sięgać aż **do 20 000 000 EUR** (słownie: dwudziestu milionów euro) lub, w przypadku przedsiębiorcy, do **4% jego rocznego światowego obrotu osiągniętego w roku poprzedzającym rok nałożenia kary**. Dodatkowym zaostrzeniem jest to, że **nakładana jest kara wyższa.**

Oznacza to, że organ będzie wyliczał karę zarówno w jednej oraz w drugiej granicy (kwotowej i procentowej). Z tych dwóch wysokości kar ostatecznie nałożona zostanie ta, która będzie wyższa.

1. Zakres odpowiedzialności administratorów

Administrator lub podmiot przetwarzający, ponoszą odpowiedzialność m. in. za:

- naruszenie przepisów dotyczących pozyskiwania zgód od dzieci;
- niezastosowanie się do zasady *privacy by design*;
- nieprzeprowadzenie DPIA, gdy jest ono wymagane;
- niezgłoszenie naruszenia ochrony danych organowi nadzorczemu;
- nieprowadzenie rejestru czynności przetwarzania.

Za te naruszenia organ wymierza karę do 10 000 000 euro lub 2% światowego rocznego obrotu, jeżeli naruszenia dopuścił się przedsiębiorca.

Za te naruszenia organ wymierza karę do **10 000 000 euro lub 2% światowego rocznego obrotu**, jeżeli naruszenia dopuścił się przedsiębiorca.

RODO przedstawia jednak drugą kategorię naruszeń, za które organ może wymierzyć karę:

- naruszenie podstawowych zasad przetwarzania danych (s. 9);
- utrudnianie lub uniemożliwianie realizacji praw osób, których dane dotyczą (s. 21);
- naruszenie przepisów o przekazaniu danych osobowych do odbiorcy w państwie trzecim.

W przypadku tej drugiej kategorii naruszeń kara wyznaczana jest w granicy wyżej już wspomnianych **20 000 000 euro lub 4% rocznego światowego obrotu osiągniętego w roku poprzedzającym rok nałożenia kary** w przypadku przedsiębiorcy. Również i tu wymierzana jest kara kwotowo wyższa.

Ponadto, RODO daje podstawę do cywilnoprawnych roszczeń osób, które poniosły szkodę w związku z poniesieniem szkody majątkowej i niemajątkowej w wyniku naruszenia zasad przetwarzania danych. Będzie to osobne źródło odpowiedzialności w odniesieniu do obecnych polskich przepisów w zakresie naruszenia dóbr osobistych (naprawa szkody niemajątkowej na podstawie art. 24 w zw. z art. 448 kc).

Zobowiązanym do naprawy szkody będzie administrator lub podmiot przetwarzający. Jeżeli **podmiotów uczestniczących w naruszeniu jest więcej, ich odpowiedzialność jest solidarna**. RODO przewiduje możliwość zwolnienia się od odpowiedzialności, jednak wyłącznie w przypadku, gdy podmiot chcący uniknąć odpowiedzialności **udowodni, że w żaden sposób nie ponosi winy za naruszenie.**

2. Kryteria ustalania wysokości kary

RODO wskazuje, jakimi kryteriami organ ma się kierować decydując, **czy karę wymierzać** oraz **miarkując jej wysokość**. Poniżej zostanie opisanych kilka z nich.

Przede wszystkim brany jest pod uwagę **charakter, waga i czas trwania naruszenia, liczba osób poszkodowanych** oraz **szkody, które te osoby poniosły.** Bez wątpienia można uznać, że organ będzie miał obowiązek inaczej traktować wycieki danych o różnym stopniu powagi. Dodatkowo, do oceny należy również uwzględnić **kategorie danych.**

Po drugie, **brana jest pod uwagę umyślność bądź nieumyślność naruszenia.** Przepisy RODO nie precyzują jednak co należy rozumieć pod pojęciami umyślności i nieumyślności. Biorąc pod uwagę represyjny charakter kar administracyjnych, można stwierdzić, że pojęcia te należy – o ile organy krajowe bądź unijne nie wydadzą w tym zakresie swoich wskazówek i zaleceń – analogicznie do ich znaczeń w prawie karnym. W takim wypadku poprzez **umyślność** należy rozumieć taką sytuację motywacyjną, w której administrator chciał podjąć działania/zaniechania będące naruszeniem prawa lub też spodziewał się, że jego działanie/zaniechanie może stanowić naruszenie prawa i się na to godził. Jako **nieumyślność** rozumie się taką sytuację, w której administrator nie mając zamiaru popełnienia czynu, popełnia go jednak na skutek niezachowania ostrożności wymaganej w danych okolicznościach, mimo że możliwość popełnienia tego czynu przewidywał albo mógł przewidzieć. Podstawą do przypisania umyślności lub nieumyślności przedsiębiorcy będącemu osobą prawną (lub jednostką organizacyjną nieposiadającą

osobowości prawnej) są działania osób nim zarządzających.

Po trzecie, organ obowiązany jest brać pod uwagę **działania administratora, mające na celu zminimalizowanie szkód poniesionych przez osoby, których dane dotyczą.**

Po czwarte, ocenie również podlega **stopień odpowiedzialności,** przez co należy rozumieć, na ile działania administratora lub podmiotu przetwarzającego przyczyniły się do naruszenia.

Po piąte – organ zobowiązany jest także brać pod uwagę **wszystkie wcześniejsze naruszenia ze strony administratora.** Tak więc (przynajmniej czysto teoretycznie) administrator dopuszczający się pierwszego naruszenia powinien być potraktowany łagodniej od „recydywisty". Ponadto uwzględniony zostanie **stopień współpracy z organem** w celu usunięcia i złagodzenia skutków naruszenia. W ramach współpracy z organem należy również uwzględnić, czy i w jakich okolicznościach administrator spełnił obowiązek zawiadomienia organu o stwierdzonym naruszeniu.

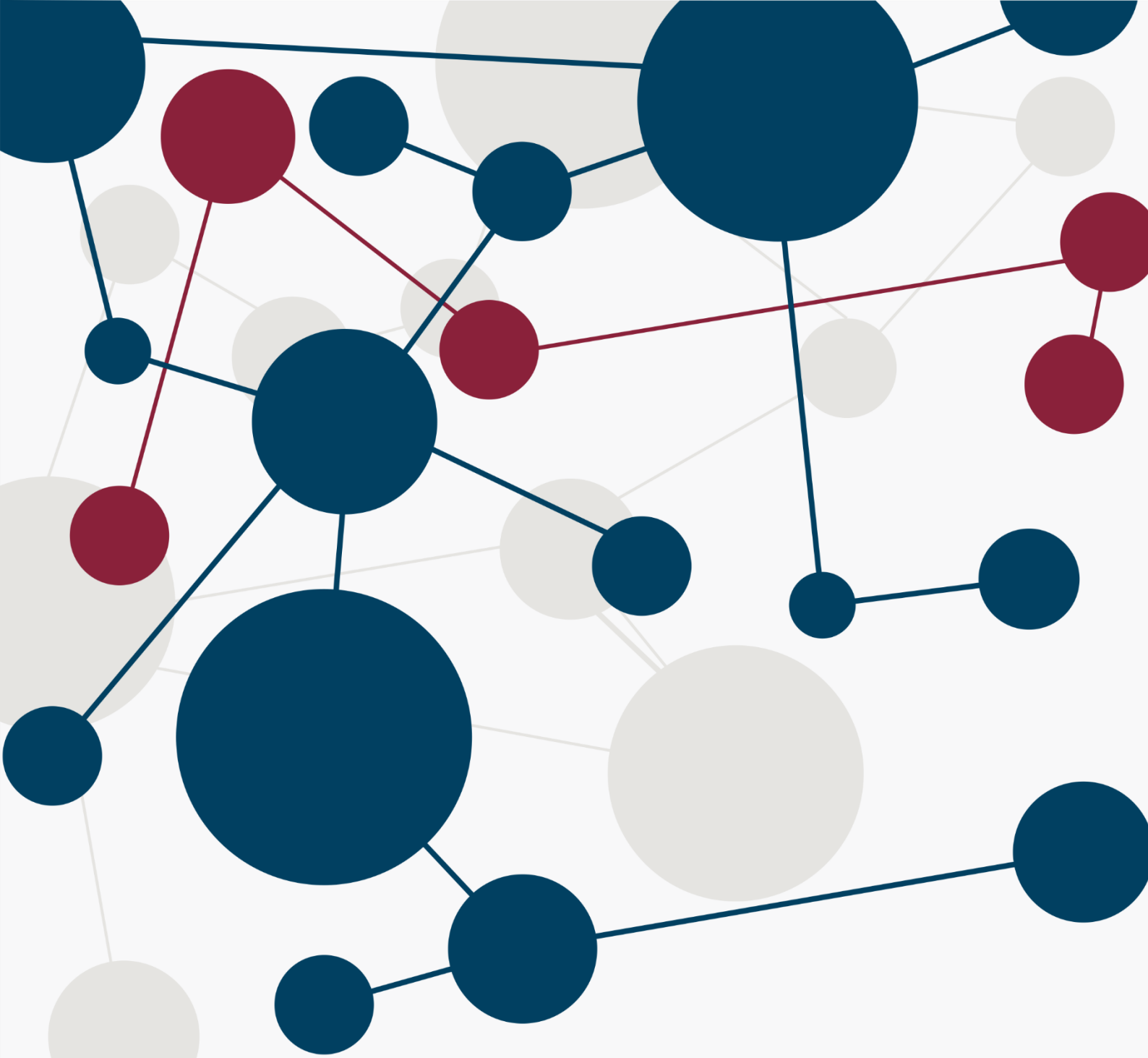
Poza szczegółowym katalogiem okoliczności wpływających na wysokość kary, organowi pozostawiono swobodę w zakresie uwzględniania **innych okoliczności obciążających lub łagodzących.**

Przykład

Spółka z o.o. przetwarza dane osobowe swoich klientów. Przechowywane są one na serwerze, który znajduje się w jej siedzibie. Z bazy korzystają jedynie pracownicy pracujący w jej siedzibie. Pomimo tego, serwer jest podłączony do Internetu, zamiast do sieci wewnętrznej i w związku z tym narażony jest na zdalne ataki. Niestety Spółka przeoczyła kwestię zainstalowania na serwerze oprogramowania zabezpieczającego, natomiast sama baza klientów nie została zabezpieczona w jakikolwiek sposób.

Grupa hakerów dokonuje ataku i wykrada dane dziesiątek tysięcy klientów (ich imiona, nazwiska, adresy, daty urodzenia itp.). O wycieku dowiaduje się krajowy organ nadzorczy z uwagi na otrzymane zawiadomienia od osób, których dane dotyczą z jednoczesną informacją o szkodach poniesionych przez te osoby. Uwzględniając taki stan faktyczny, organ powinien jako podstawę do ustalania kary zastosować wymiar kary do 10 mln EUR i do 2% łącznego światowego obrotu przedsiębiorstwa. Są to bowiem naruszenia dotyczące należytego zabezpieczenia przetwarzanych danych osobowych. Z uwagi na istotne braki w tym zakresie, brak podjęcia działań minimalizujących konsekwencje naruszenia, w tym brak poinformowania osób, których dane dotyczą, wysokość kary nałożonej na przedsiębiorcę może być znaczna.

Dodatkowo osoby, których dane dotyczą, na podstawie RODO będą kierowały przeciwko Spółce powództwa o zapłatę odszkodowania, w tym zadośćuczynienia za doznaną krzywdę.



RODO 2018

wprowadzenie do zmian

Zakończenie

Zakończenie

Podsumowując, regulacja RODO wprowadza bardziej praktyczne niż dotychczasowe przepisy o ochronie danych.

Faktem jest, że RODO w istocie stanowi reakcję na zmiany w rzeczywistości społeczno-gospodarczej. Przyjęte rozwiązania są w większości przypadków dostosowane do społeczeństwa bazującego na elektronicznym przepływie informacji, gdzie większym zagrożeniem jest uzyskanie dostępu do serwerów danej korporacji i danych tam zawartych niż dostęp do pomieszczeń czy biur takiego podmiotu.

RODO wymusza na administratorze samodzielne podejmowanie decyzji, co do tego jak zabezpieczać dane osobowe. RODO słusznie eliminuje powszechny obowiązek zgłaszania zbiorów danych osobowych do rejestrów organów nadzorczych w państwach członkowskich. Również istotną korzyścią jest fakt, że akt ten obowiązuje na terytorium całej Unii Europejskiej zatem ewentualne różnice między państwami członkowskimi w zakresie przetwarzania danych osobowych będą niewielkie.

Istotnym problemem jest natomiast natłok obowiązków informacyjnych spoczywających na administratorze, któremu trudno będzie im sprostać. Co więcej osoba, której dane dotyczą, będzie zalewana informacjami, z których może nic nie zrozumieć lub których po prostu nie będzie czytać. Dodatkowo Autorzy mają wątpliwości, czy zasada rozliczalności (obowiązek wykazania, że dane osobowe są przetwarzane zgodnie z prawem) nie weźmie góry nad faktycznym obowiązkiem należytego przetwarzaniem danych osobowych. Wątpliwości wzbudza również sposób, w jaki administratorzy wprowadzą u siebie regulacje dotyczące przenaszalności danych osobowych.

Trudnym do spełnienia dla administratorów obowiązkiem może również okazać się zgłaszanie organowi nadzorczemu naruszenia ochrony danych oraz zawiadamiania osób, których dane dotyczą o naruszeniu ochrony danych.

Odnosząc się natomiast do bardzo istotnej zmiany, która ma miejsce w stosunku do dotychczasowych przepisów, czyli przyznania organowi nadzorczemu kompetencji do nakładania kar pieniężnych na podmioty naruszające przepisy o ochronie danych, niewątpliwie należy stwierdzić, że to właśnie dzięki tej zmianie wiele podmiotów zainteresuje się uregulowaniem kwestii ochrony danych. Nie zmienia to jednak faktu, że wszystkie podmioty będą zobowiązane do dostosowania sposobu, w jaki przetwarzają dane osobowe, gdyż jeden z góry określony sposób zabezpieczenia danych osobowych nie będzie już obowiązywał.

Wszystkie powyżej zauważone kwestie prowadzą do wniosku, że każdy administrator oraz podmiot przetwarzający dane powinien wygospodarować czas na należyte zajęcie się tematem prawidłowego wdrożenia RODO do swojej organizacji.

Takie działanie zwiększy poczucie bezpieczeństwa administratora lub podmiotu przetwarzającego i jednocześnie uchroni, a co najmniej zminimalizuje ryzyko naruszenia interesów osób, których dane dotyczą, a także ryzyko nałożenia kar pieniężnych.

Mateusz Oskroba
radca prawny

Kancelaria Prawna
Piszcz i Wspólnicy
mateusz.oskroba@piszcz.pl
Tel: +48 609 055 570
Tel: +48 61 859 44 44

Łukasz Zboralski
radca prawny

Kancelaria Prawna
Piszcz i Wspólnicy
lukasz.zboralski@piszcz.pl
Tel: +48 61 859 44 44

RODO 2018

Zapraszamy do kontaktu