

Toruń, dnia 25 maja 2018 r.

Procedury dotyczące ochrony danych osobowych

DRIMER Sp. z o.o. sp.k. z siedzibą w Toruniu

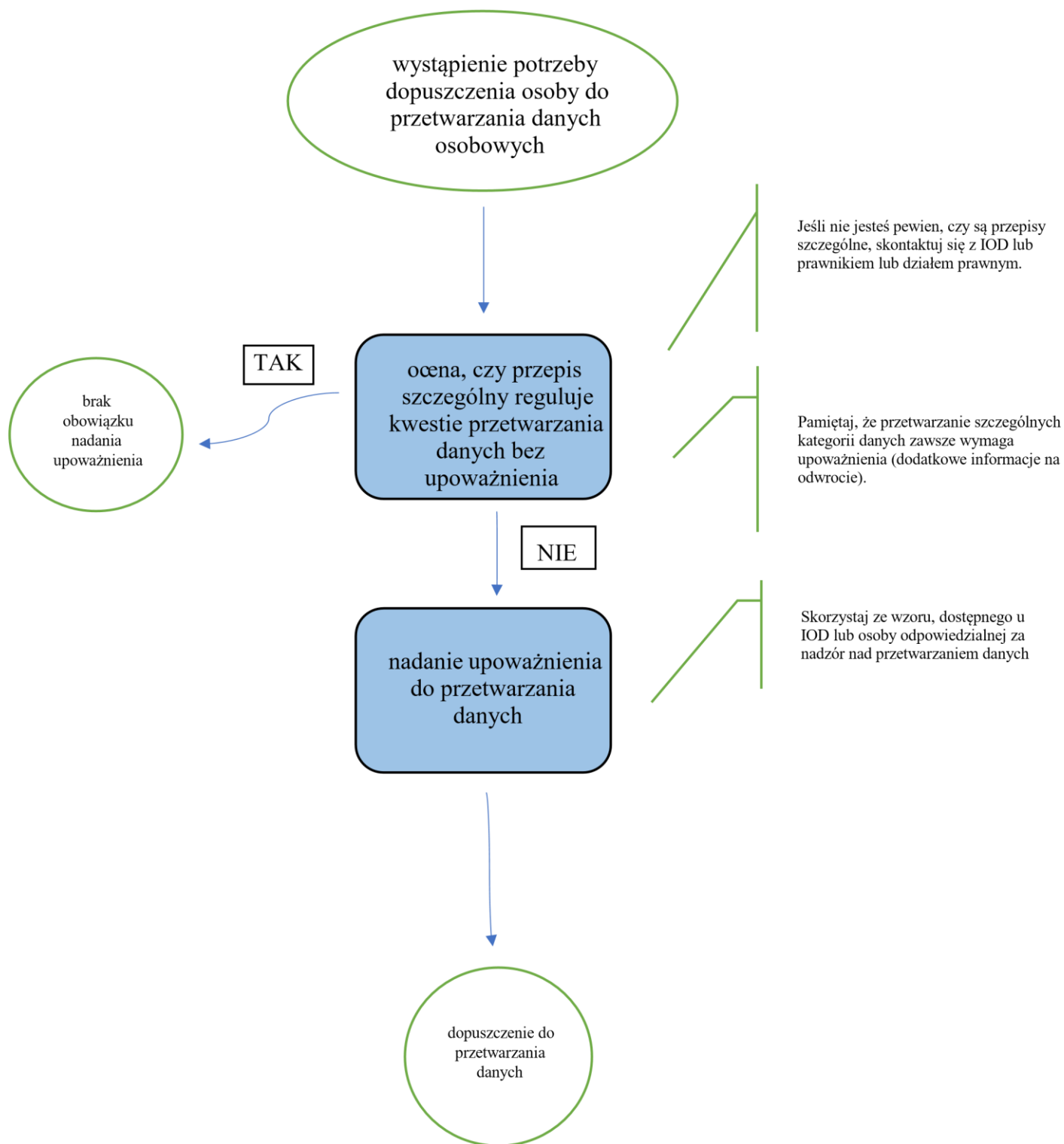
Szanowni Państwo,

w niniejszym dokumencie znajdują Państwo opis obowiązujących w Spółce procedur postępowania w istotnych sprawach z punktu widzenia ochrony danych osobowych, w tym związanych z realizacją swoich uprawnień przez osoby, których dane dotyczą. Procedury te odzwierciedlają zmiany w prawie ochrony danych osobowych dokonane na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – zwanym dalej RODO.

Spis treści

I.	NADAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH	1
II.	POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH	4
III.	OBOWIĄZEK INFORMACYJNY ZGODNIE Z RODO	7
IV.	OBOWIĄZEK PROWADZENIA REJESTRU CZYNNOŚCI PRZETWARZANIA	9
V.	OBOWIĄZEK PRZEPROWADZENIA OCENY SKUTKÓW DLA OCHRONY DANYCH	13
VI.	POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH	15
VII.	PRAWO DO OGRANICZENIA PRZETWARZANIA, USUNIĘCIA I SPROSTOWANIA DANYCH	19
VIII.	PRAWO DO ŻĄDANIA OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH	21
IX.	PRAWO DO ŻĄDANIA SPROSTOWANIA LUB UZUPEŁNIENIA DANYCH OSOBOWYCH	23
X.	PRAWO DO ŻĄDANIA USUNIĘCIA DANYCH OSOBOWYCH („PRAWO DO BYCIA ZAPOMNIANYM”)	25
XI.	POSTĘPOWANIE W PRZYPADKU WNIESIENIA SPRZECIWU PRZEZ OSOBĘ, KTÓREJ DANE DOTYCZĄ	28
XII.	WNIOSEK OSOBY, KTÓREJ DANE DOTYCZĄ O PRZENIESIENIE DANYCH OSOBOWYCH	31
XIII.	WNIOSEK OD OSOBY, KTÓREJ DANE DOTYCZĄ O UDZIELENIE INFORMACJI	33
XIV.	OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH OSOBOWYCH	35

administrator, podmiot przetwarzający



Przetwarzanie szczególnych kategorii danych zawsze wymaga upoważnienia. Zabrania się przetwarzania danych osobowych ujawniających **pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.**

Powyższe nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

- a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
- b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
- h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
- i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
- j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia Spółki lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je **wyłącznie na polecenie Spółki, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.**

Jeżeli wystąpi potrzeba dopuszczenia osoby do przetwarzania danych osobowych, należy ustalić, czy przepis szczególny reguluje kwestie przetwarzania danych bez upoważnienia. Jeśli tak, to nie ma obowiązku nadawania upoważnienia. Jeśli jednak nie, należy nadać upoważnienie do przetwarzania danych.

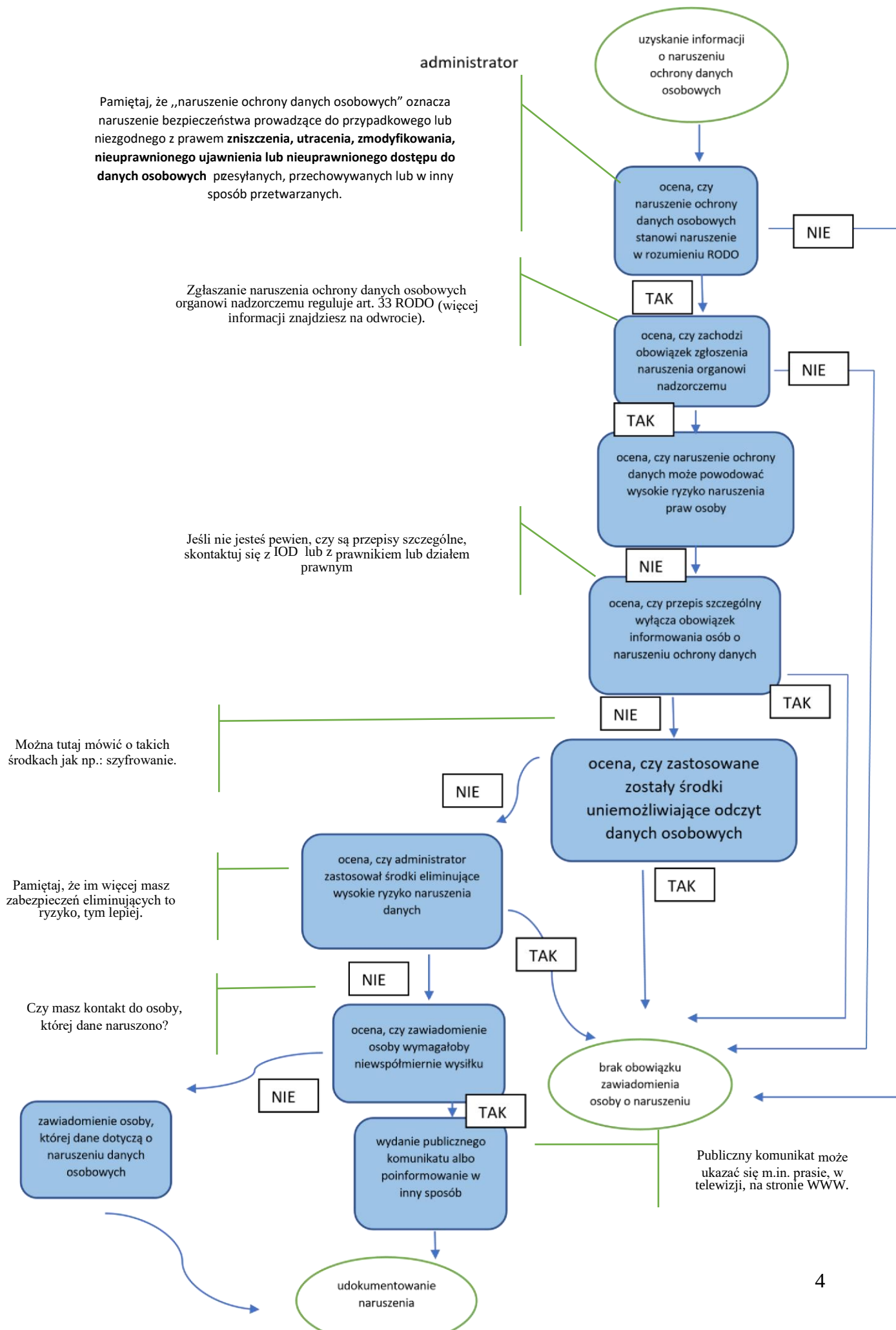
Jeżeli przetwarzanie ma być dokonywane w imieniu Spółki, korzysta ona wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa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

Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i Spółkę, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

- a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
- b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- c) podejmuje wszelkie środki wymagane na mocy art. 32;
- d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;
- e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;
- f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;
- g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
- h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje Spółkę, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

II. POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH



W momencie uzyskania informacji o naruszeniu ochrony danych osobowych, w pierwszej kolejności należy ocenić, czy naruszenie ochrony danych osobowych stanowi naruszenie w rozumieniu RODO. Zgodnie z RODO „*naruszenie ochrony danych osobowych*” oznacza *naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych*.

Jeżeli doszło do takiego naruszenia to należy czy ocenić, czy zachodzi obowiązek zgłoszenia naruszenia organowi nadzorczemu.

Artykuł 33. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu.

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, **chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Jeżeli zachodzi obowiązek zgłoszenia naruszenia organowi nadzorczemu, należy ocenić, czy naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw osoby. Jeśli nie, w dalszej kolejności oceniamy, czy przepis szczególny wyłącza obowiązek informowania osób o naruszeniu ochrony danych. Jeśli tak- brak obowiązku zawiadomienia osoby o naruszeniu.

Jeśli nie, należy ocenić, czy zastosowane zostały środki uniemożliwiające odczyt danych osobowych. Jeśli tak- brak obowiązku zawiadomienia osoby o naruszeniu. Jeśli nie, oceniamy, czy administrator zastosował środki eliminujące wysokie ryzyko naruszenia danych (np. szyfrowanie, zamykane szafki). Jeśli tak- brak obowiązku zawiadomienia osoby o naruszeniu.

Jeśli administrator nie zastosował środków eliminujących wysokie ryzyko naruszenia danych, należy ocenić, czy zawiadomienie osoby wymagałoby niewspółmiernie wysiłku. Jeśli nie, to daną osobę należy zawiadomić. Jeżeli jednak jest to utrudnione, poinformować o naruszeniu można poprzez wydanie publicznego komunikatu (np. w prasie, telewizji). W dalszej kolejności następuje udokumentowanie naruszenia.

administrator

Pamiętaj, że zgodnie z RODO, „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem **zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu** do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

uzyskanie informacji o
naruszeniu przepisów o
ochronie danych
osobowych

ocena, czy naruszenie
przepisów stanowi
naruszenie ochrony danych
osobowych w rozumieniu
RODO

TAK

ocena, czy naruszenie
ochrony danych skutkuje
ryzykiem naruszenia praw
osoby

TAK

zgłoszenia naruszenia
ochrony danych
organowi nadzorczemu

ocena, czy wymagane jest
zawiadomienie osoby,
której dane dotyczą o
naruszeniu

udokumentowanie
naruszenia

NIE

NIE

brak obowiązku
zgłoszenia
naruszenia
organowi
nadzorczemu

Zgłaszanie naruszenia ochrony danych
osobowych organowi nadzorczemu reguluje
art. 33 RODO (więcej informacji na odwrocie)

III. OBOWIĄZEK INFORMACYJNY ZGODNIE Z RODO

Informowanie osób, których dane dotyczą o przetwarzaniu ich danych osobowych, stanowi jeden z podstawowych obowiązków Spółki jako administratora danych. Obowiązek informacyjny **aktualizuje się w trzech sytuacjach**:

- przy zbieraniu danych, od osoby, której dane dotyczą;
- przy zbieraniu danych w sposób inny niż od osoby, której dane dotyczą;
- przez cały okres przetwarzania danych osobowych (w związku z prawem dostępu przysługującym osobie, której dane dotyczą).

W przypadku wystąpienia potrzeby zebrania danych osobowych, należy w pierwszej kolejności ustalić, od kogo dane osobowe mają być zebrane. W przypadku jeśli mają być zebrane z tzw. innych źródeł, należy ustalić, czy przepis szczególny wyłącza obowiązek informowania o zbieraniu danych. Jeśli tak- brak obowiązku informacyjnego. Jeśli nie, w dalszej kolejności ustalamy, czy udzielenie informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Jeśli tak- brak obowiązku informacyjnego.

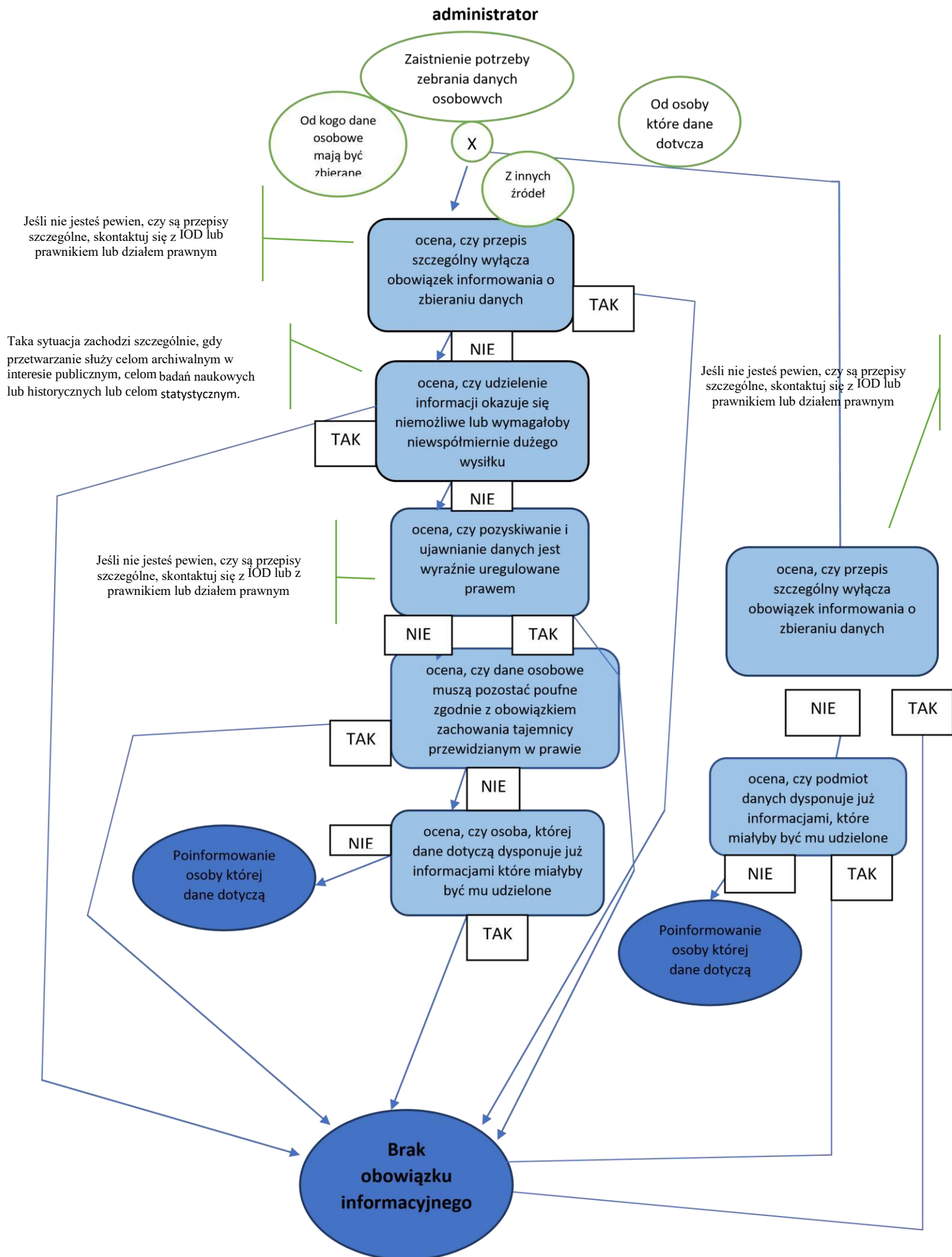
Zgodnie z RODO, „sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia.”

Jeśli nie, następnie ustalamy, czy pozyskiwanie i ujawnianie danych jest wyraźnie uregulowane prawem. Jeśli tak- brak obowiązku informacyjnego.

Jeżeli nie jest uregulowane prawem, należy ocenić, czy żądania są ewidentnie nieuzasadnione lub nadmierne. *Chodzi tu w szczególności o sytuacje, gdzie żądanie jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.* Jeśli tak- brak obowiązku informacyjnego.

Jeżeli nie jest nieuzasadnione lub nadmierne, na sam koniec należy ocenić, czy osoba, której dane dotyczą dysponuje już informacjami, które miałyby być mu udzielone. Jeśli nie, to należy ją poinformować o zebranych danych osobowych.

Inna procedura obowiązuje w sytuacji, gdy dane osobowe mają być zebrane od osoby, której dotyczą. Wtedy w pierwszej kolejności oceniamy, czy przepis szczególny wyłącza obowiązek informowania o zbieraniu danych. Jeżeli wyłącza, to nie mamy obowiązku informacyjnego. Jeśli nie wyłącza, w dalszej kolejności oceniamy, czy podmiot danych dysponuje już informacjami, które miałyby być mu udzielone. Jeśli dysponuje to również nie mamy obowiązku informacyjnego. W przeciwnym razie, poinformowanie jest konieczne.



IV. OBOWIĄZEK PROWADZENIA REJESTRU CZYNNOŚCI PRZETWARZANIA

Spółka oraz – gdy ma to zastosowanie – przedstawiciel Spółki **prowadzą** rejestr czynności przetwarzania danych osobowych, za które odpowiadają. Obowiązek ten co do zasady nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Artykuł 9. RODO

Przetwarzanie szczególnych kategorii danych osobowych.

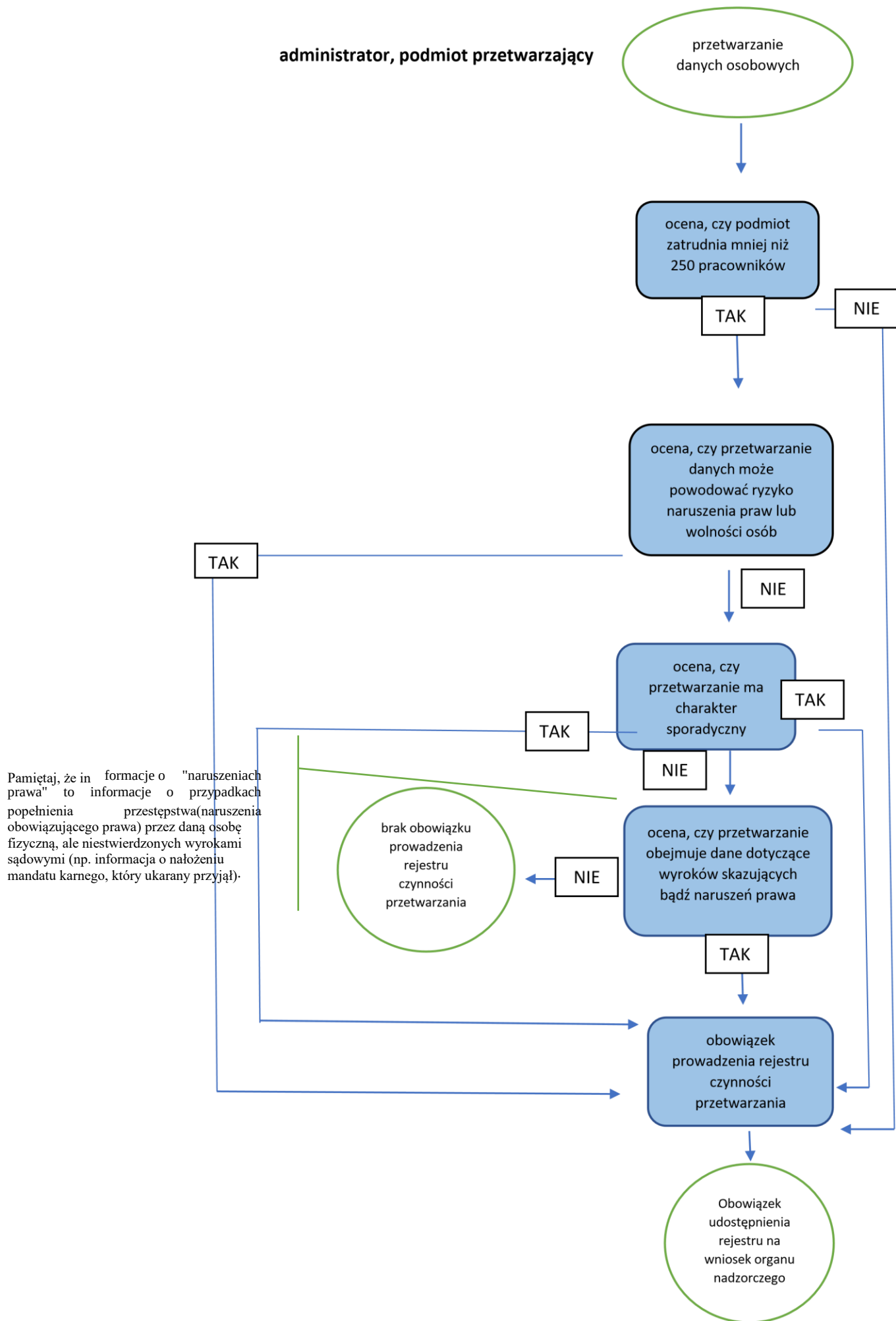
Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

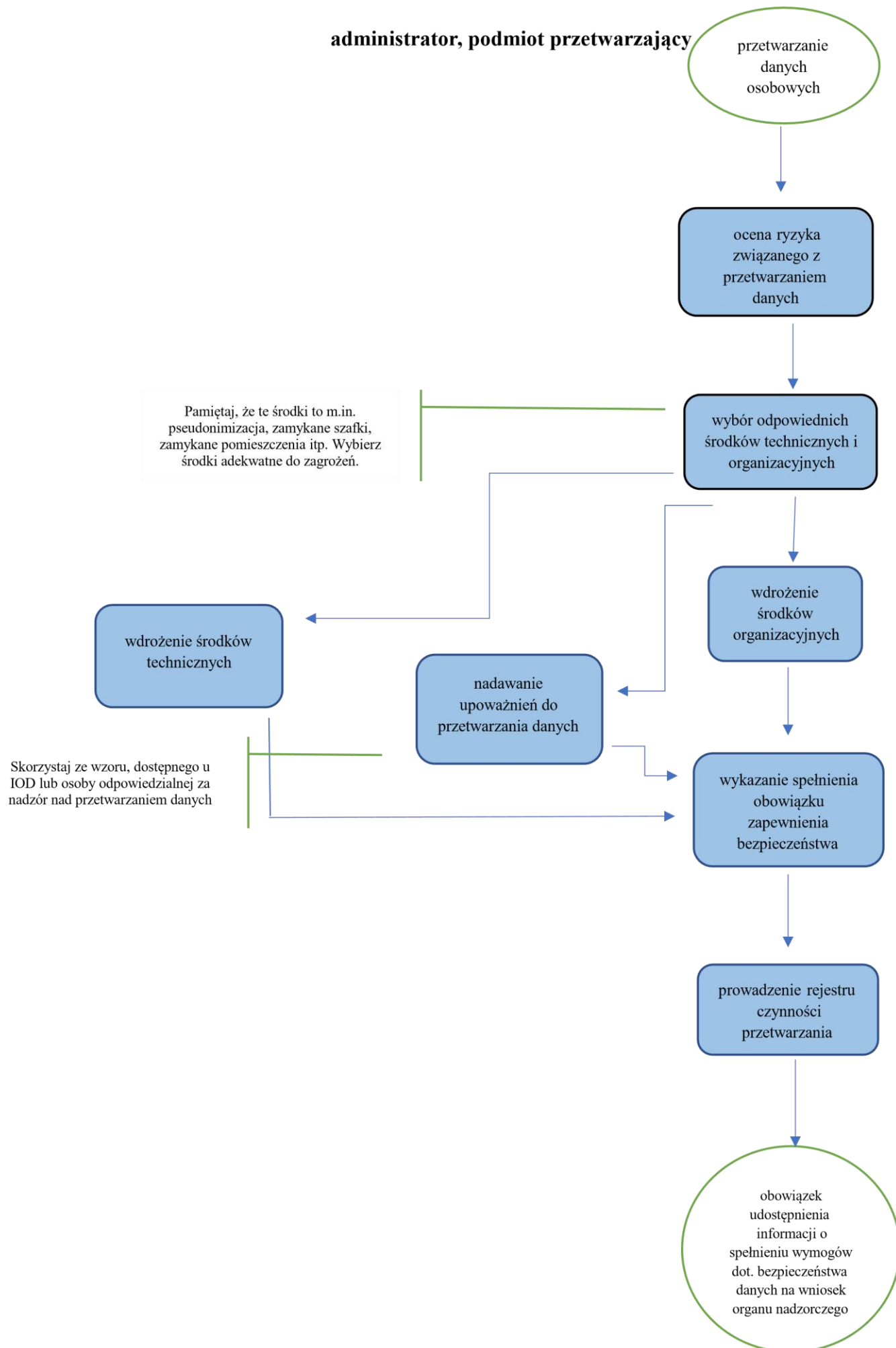
Artykuł 10. RODO

Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Rejestr podlega udostępnieniu organu nadzorczemu na jego wniosek.





W pierwszej kolejności należy ocenić ryzyko, związane z przetwarzaniem danych osobowych. Co do zasady ryzyko można podzielić na biznesowe oraz operacyjne. Ryzyko biznesowe to możliwość poniesienia strat w wyniku niewłaściwych decyzji co do doboru klientów, kształtu produktów i usług lub zobowiązań wobec partnerów biznesowych albo w wyniku niesprawności lub niespójności systemu społeczno-gospodarczego państwa. Ryzyko operacyjne to ryzyko strat w wyniku niewłaściwego lub błędnego działania procesu, ludzi i systemów albo wpływu zagrożeń zewnętrznych.

W dalszej kolejności, należy dokonać wyboru odpowiednich środków technicznych i organizacyjnych. Te środki to m.in. pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. Po wybraniu odpowiednich środków, następuje ich wdrożenie. Tym samym następuje spełnienie obowiązku zapewnienia bezpieczeństwa. Wiąże się to z prowadzeniem rejestru przetwarzania oraz z obowiązkiem udostępnienia informacji o spełnieniu wymogów dot. bezpieczeństwa danych na wniosek organu nadzorczego.

V. OBOWIĄZEK PRZEPROWADZENIA OCENY SKUTKÓW DLA OCHRONY DANYCH

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Spółka przed rozpoczęciem przetwarzania dokonuje **oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych**. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Jeśli ocena skutków dla ochrony danych została przeprowadzona w ramach prac legislacyjnych, nie ma obowiązku przeprowadzenia oceny skutków dla ochrony danych. Jeżeli jednak ocena skutków dla ochrony danych nie została przeprowadzona w ramach prac legislacyjnych, należy sprawdzić, czy dany rodzaj przetwarzania podlega obowiązkowej ocenie skutków (przetwarzanie polegające w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych). Jeżeli nie, to należy ocenić, czy dany rodzaj przetwarzania został wskazany jako niepodlegający ocenie skutków. Jeśli został - brak obowiązku przeprowadzenia oceny skutków dla ochrony danych.

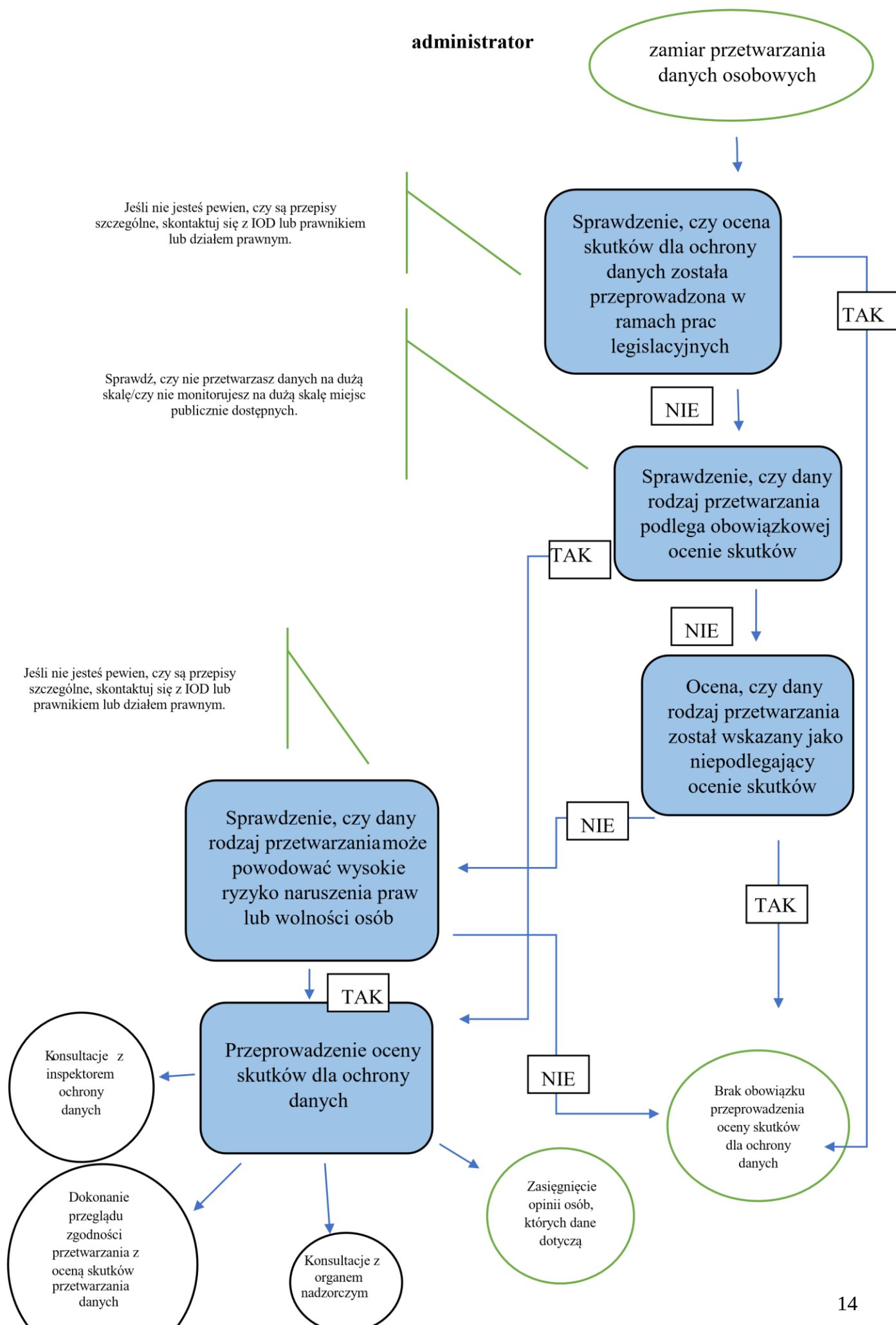
Jeżeli dany rodzaj przetwarzania nie został wskazany jako niepodlegający ocenie skutków, należy sprawdzić, czy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób.

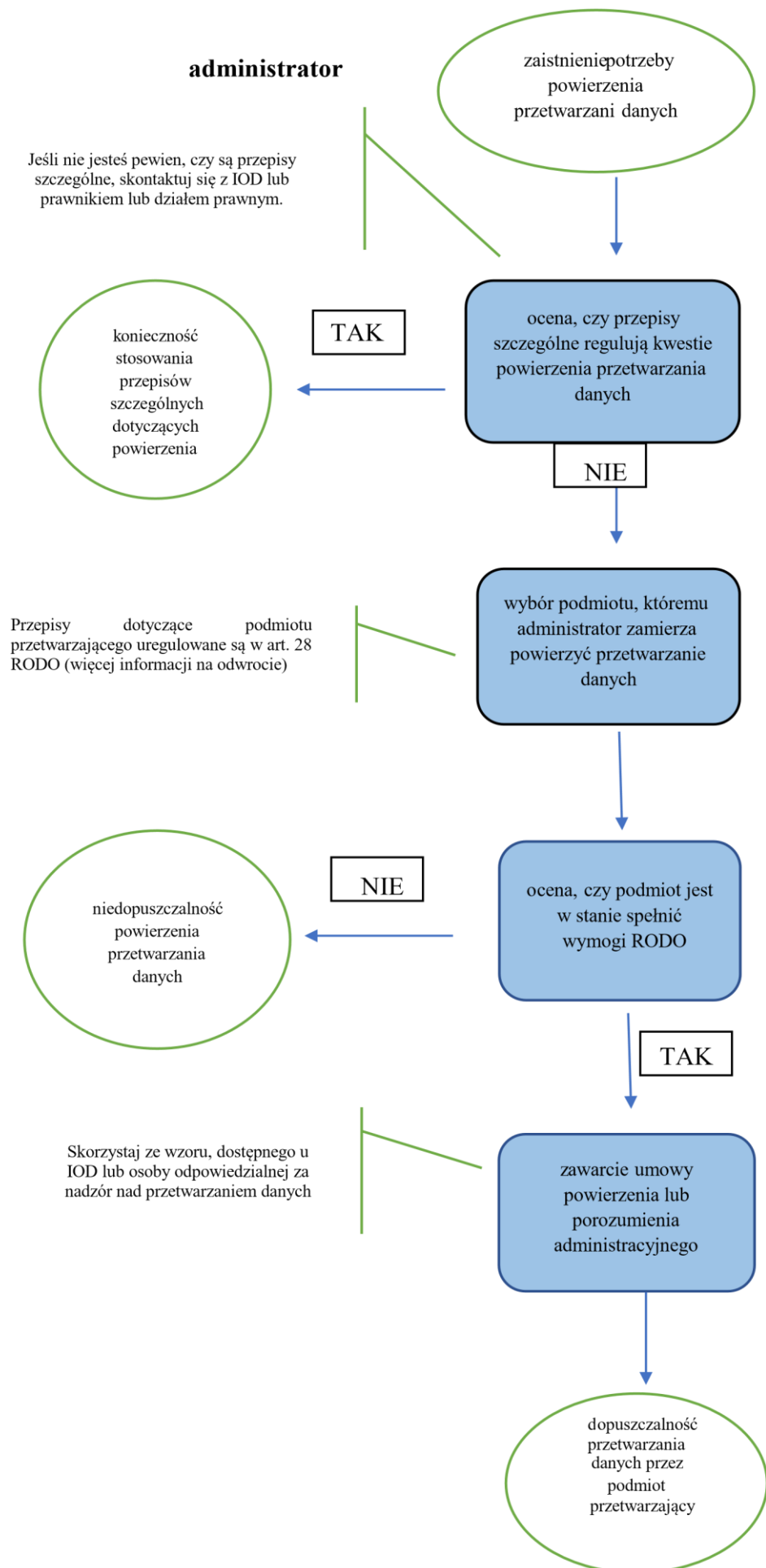
Jeżeli ocena skutków dla ochrony danych wykaże, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a Spółka wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym. Takie wysokie ryzyko mogą powodować pewne rodzaje przetwarzania oraz zakres i częstotliwość przetwarzania, które mogą skutkować także szkodą lub ingerencją w prawa i wolności osoby fizycznej.

Jeśli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób, należy przeprowadzić ocenę skutków dla ochrony danych. Ocena skutków związana jest z:

- a) konsultacjami z inspektorem ochrony danych,
- b) dokonaniem przeglądu zgodności przetwarzania z oceną skutków przetwarzania danych,
- c) konsultacjami z organem nadzorczym,
- d) zasięgnięciem opinii osób, których dane dotyczą.

administrator





W momencie zaistnienia potrzeby powierzenia przetwarzania danych, w pierwszej kolejności należy ocenić, czy przepisy szczególne regulują kwestie powierzenia przetwarzania danych. Jeśli tak, to mamy konieczność stosowania przepisów szczególnych dotyczących powierzenia.

Jeśli nie ma przepisów szczególnych, następuje wybór podmiotu, któremu administrator zamierza powierzyć przetwarzanie danych. Aby mogło dojść do skutecznego powierzenia przetwarzania, podmiot musi spełniać wymogi, zgodnie z RODO. Zgodnie z definicją rozporządzenia, *podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.*

Artykuł 28. Podmiot przetwarzający.

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

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

3. *Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowi w szczególności, że podmiot przetwarzający:*

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny; b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy; c) podejmuje wszelkie środki wymagane na mocy art. 32;

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;

e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

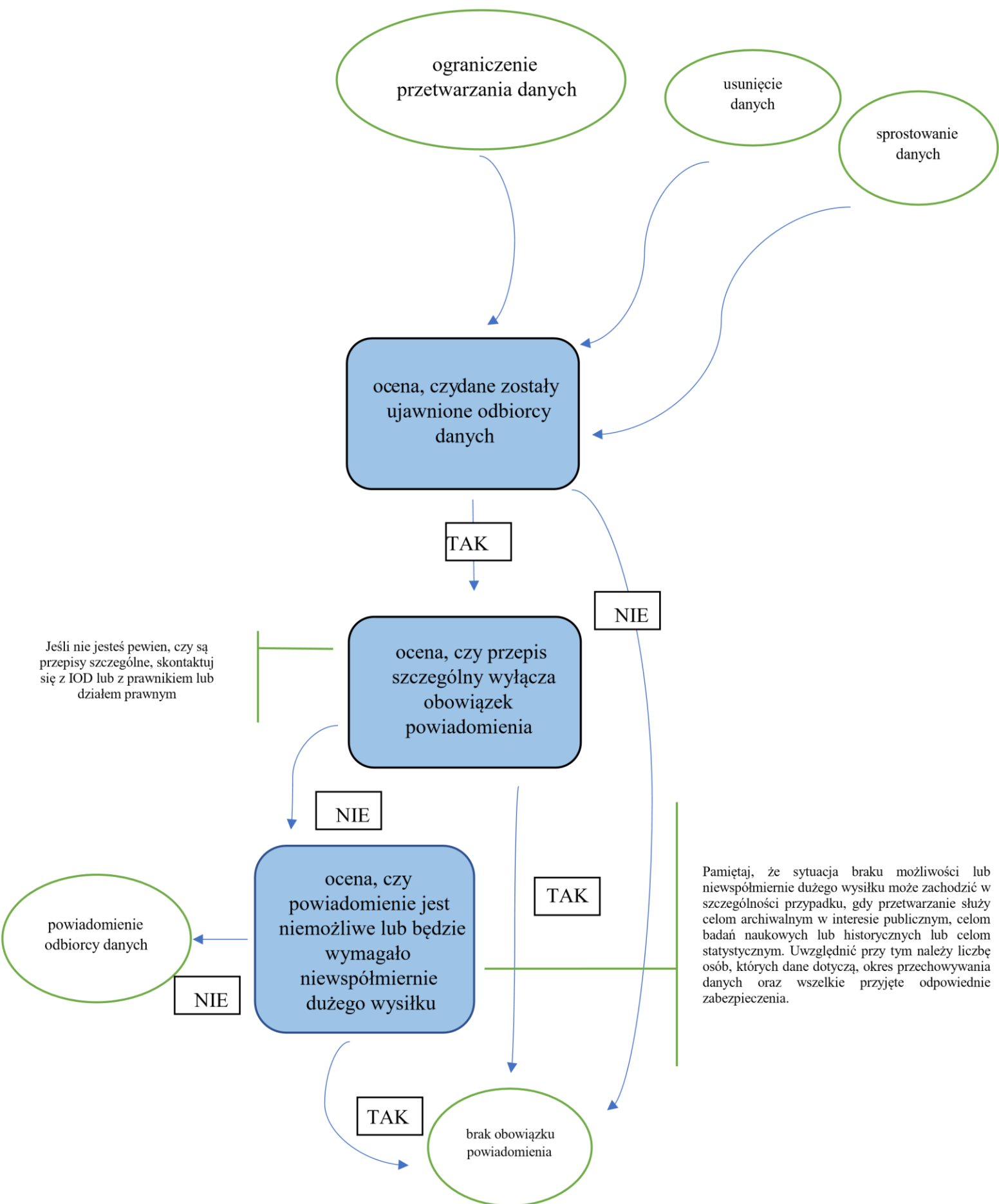
W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

4. *Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec*

- administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.*
- 5. Wystarczające gwarancje, o których mowa w ust. 1 i 4 niniejszego artykułu, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.*
 - 6. Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 3 i 4 niniejszego artykułu, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 7 i 8 niniejszego artykułu, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43.*
 - 7. Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.*
 - 8. Organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z mechanizmem spójności, o którym mowa w art. 63.*
 - 9. Umowa lub inny akt prawny, o których mowa w art. 3 i 4, mają formę pisemną, w tym formę elektroniczną.*
 - 10. Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.*

Jeżeli podmiot spełnia ww. wymogi, następuje zawarcie umowy powierzenia lub porozumienia administracyjnego.

administrator



Administrator odpowiada za zgodność przetwarzania danych z zasadami wynikającymi z rozporządzenia, za realizację żądań osób, których dane dotyczą, wynikających z przepisów art. 15–22 RODO, a także jest obciążony pełną odpowiedzialnością za przetwarzanie danych, które prowadzi samodzielnie lub które prowadzone jest w jego imieniu.

Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15– 22 RODO (ograniczenie przetwarzania danych, usunięcie danych, sprostowanie danych).

Artykuł 11. RODO Przetwarzanie niewymagające identyfikacji.

1. Jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia.

2. Jeżeli w przypadkach, o których mowa w ust. 1 niniejszego artykułu, administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. **W takich przypadkach zastosowania nie mają art. 15–20, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować.**

Zatem, jeżeli dane nie zostały ujawnione odbiorcy danych, administrator nie ma obowiązku powiadomienia. Jeżeli jednak dane zostały ujawnione odbiorcy danych, należy ustalić, czy przepis szczególny wyłącza obowiązek powiadomienia. Jeśli wyłącza, to administrator także nie ma obowiązku powiadomienia. Jeśli natomiast nie ma takiego przepisu to należy ocenić, czy powiadomienie jest niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku.

Zgodnie z RODO, „sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia.”

Jeżeli powiadomienie jest niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku, to administrator również nie ma obowiązku powiadomienia. Jeśli jednak nie jest ono niemożliwe, a także nie będzie wymagało niewspółmiernie dużego wysiłku, na administratorze ciąży obowiązek powiadomienia odbiorcy danych.

DEFINICJE

- „ograniczenie przetwarzania” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,
- Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia

Osoba, której dane dotyczą, może żądać ograniczenia przetwarzania danych osobowych. Po odebraniu żądania, administrator ocenia, czy uprawnienia do żądania ograniczenia przetwarzania zostało wyłączone na mocy przepisów szczególnych. Jeśli tak, nie trzeba spełniać żądania. Jeśli jednak nie, należy ocenić, czy osoba, której dane dotyczą kwestionuje prawidłowość danych, i żąda ograniczenia przetwarzania. Jeśli tak – automatycznie oceniamy, czy żądania są nadmierne albo ewidentnie nieuzasadnione.

Jeśli nie – w dalszej kolejności oceniamy, czy przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych. Jeśli tak – automatycznie oceniamy, czy żądania są nadmierne albo ewidentnie nieuzasadnione.

Jeśli nie, oceniamy, czy administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń. Jeśli tak – automatycznie oceniamy, czy żądania są nadmierne albo ewidentnie nieuzasadnione.

Jeśli nie, należy ocenić, czy osoba której dane dotyczą, wniosła sprzeciw. Jeżeli nie wniosła, to administrator nie musi spełniać żądania. Jeśli jednak sprzeciw został wniesiony, oceniamy, czy żądania są nadmierne albo ewidentnie nieuzasadnione.

Prawodawca ma na myśli w szczególności sytuacje, gdzie żądania jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.

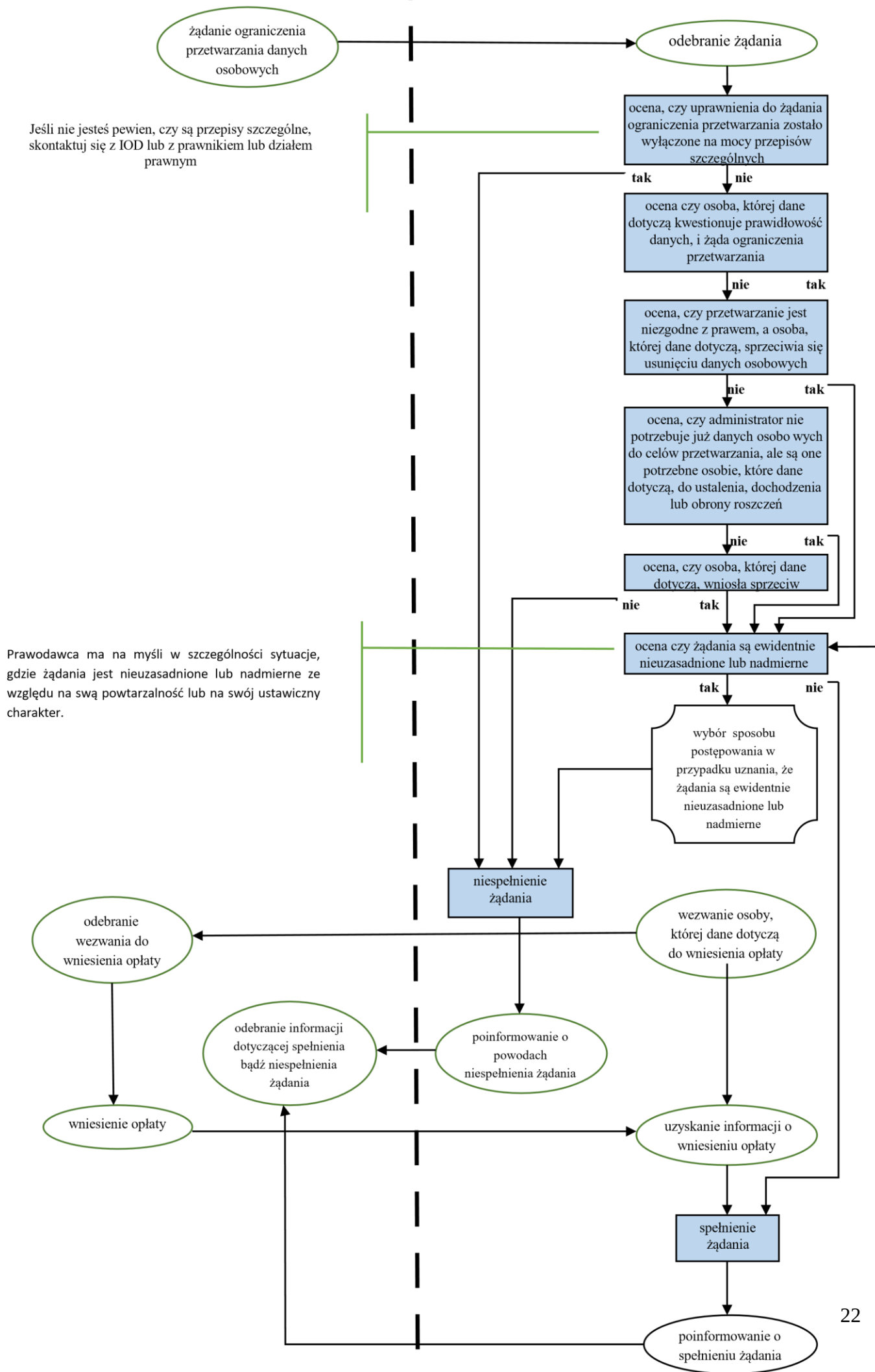
Zgodnie z RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo
- b) odmówić podjęcia działań w związku z żądaniem.

Po uzyskaniu informacji o wniesieniu opłaty, następuje realizacja wniosku i poinformowanie o spełnieniu żądania.

Z RODO...

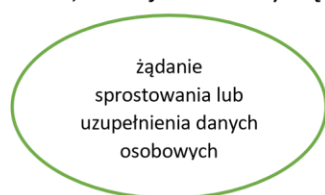
„ograniczenie przetwarzania” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania



IX. PRAWO DO ŻĄDANIA SPROSTOWANIA LUB UZUPEŁNIENIA DANYCH OSOBOWYCH

osoba, której dane dotyczą

administrator



Jeśli nie jesteś pewien, czy są przepisy szczególne, skontaktuj się z IOD lub z prawnikiem lub działem prawnym

Czy jest konieczne, żebyś przetwarzał te dane?

Prawodawca ma na myśli w szczególności sytuacje, gdzie żądania jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.

odebranie
żądania

ocena, czy spełnienie
żądania jest regulowane
przepisami szczególnymi

TAK

NIE

uzupełnienie danych

ocena, czy dane osobowe są
błędne, nieaktualne lub w inny
sposób nieprawidłowe

sprostowanie danych

NIE

TAK

ocena, czy dane są
niekompletne

ocena konieczności
przetwarzania
danych

TAK

NIE

wybór sposobu
postępowania w
przypadku uznania,
że żądania są
ewidentnie
nieuzasadnione lub
nadmierne

ocena, czy żądania
są ewidentnie
nieuzasadnione lub
nadmierne

TAK

NIE

niepełnienie żądania

wezwanie osoby,
której dane
dotyczą do
wniesienia opłaty

odebranie
wezwania do
wniesienia

poinformowanie o
powodach
niespełnienia żądania

uzyskanie
informacji o
wniesieniu opłaty

odebranie informacji
dotyczącej spełnienia
bądź niespełnienia
żądania

wniesienie
opłaty

spełnienie
żądania

23

poinformowanie o
spełnieniu żądania

Osoba, której dane dotyczą, może żądać sprostowania lub uzupełnienia danych osobowych. Po odebraniu żądania, administrator ocenia, czy spełnienie żądania jest regulowane przepisami szczególnymi. Jeśli tak, to automatycznie prowadzi to do niezrealizowania żądania. Jeśli nie, to należy ocenić, czy dane osobowe są błędne, nieaktualne lub w inny sposób nieprawidłowe. Jeśli okaże się, że będą, to w następnej kolejności należy ocenić, czy istnieje konieczność przetwarzania tych danych (może administrator już ich nie potrzebuje?). Jeśli istnieje taka potrzeba, oceniamy czy żądania są ewidentnie nieuzasadnione lub nadmierne.

Prawodawca ma na myśli w szczególności sytuacje, gdzie żądania jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.

Zgodnie z RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo
- b) odmówić podjęcia działań w związku z żądaniem.

Po uzyskaniu informacji o wniesieniu opłaty, następuje realizacja wniosku i poinformowanie o realizacji wniosku.

Z RODO...

Artykuł 16. Prawo do sprostowania danych.

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Artykuł 19. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania.

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

X. PRAWO DO ŻĄDANIA USUNIĘCIA DANYCH OSOBOWYCH („PRAWO DO BYCIA ZAPOMNIANYM”)

Osoba, której dane dotyczą, może żądać usunięcia jej danych osobowych („prawo do bycia zapomnianym”). Po odebraniu żądania, administrator ocenia, czy dane nie są już niezbędne do realizacji celów. Jeśli tak – automatycznie oceniamy, czy przetwarzanie jest niezbędne do korzystania z prawa do wolności i informacji.

Jeśli nie – oceniamy, czy osoba, której dane dotyczą cofnęła zgodę. Jeśli tak – automatycznie oceniamy, czy przetwarzanie jest niezbędne do korzystania z prawa do wolności i informacji. Jeśli cofnięcie zgody nie nastąpiło, należy sprawdzić, czy osoba, której dane dotyczą, wniosła sprzeciw. Jeśli tak – automatycznie oceniamy, czy przetwarzanie jest niezbędne do korzystania z prawa do wolności i informacji.

Jeśli nie mamy sprzeciwu, oceniamy czy dane były przetwarzane niezgodnie z prawem. Jeśli tak – automatycznie oceniamy, czy przetwarzanie jest niezbędne do korzystania z prawa do wolności i informacji.

Jeśli dane były przetwarzane zgodnie z prawem, sprawdzamy czy dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego. W przypadku jeśli nie muszą, sprawdzamy, czy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego. Jeśli nie – nie musimy spełniać żądania usunięcia danych.

Jeśli tak, oceniamy czy przetwarzanie jest niezbędne do korzystania z prawa do wolności i informacji. Jeśli tak – nie musimy spełniać żądania usunięcia danych.

Jeśli nie, to w następnej kolejności, sprawdzamy, czy przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku lub wykonania zadania realizowanego w interesie publicznym bądź w ramach sprawowania władzy publicznej. Jeśli tak – nie musimy spełniać żądania usunięcia danych.

Jeśli nie, oceniamy, czy przetwarzanie jest niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego. Jeśli tak – nie musimy spełniać żądania usunięcia danych.

Jeśli nie, w dalszej kolejności sprawdzamy, czy przetwarzanie jest niezbędne do celów archiwalnych, badań naukowych, historycznych lub statystycznych. Jeśli tak – nie musimy spełniać żądania usunięcia danych.

Jeśli nie jest, oceniamy, czy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń. Jeśli tak – nie musimy spełniać żądania usunięcia danych.

Jeśli nie jest nam do tego niezbędne, oceniamy, czy żądania są nadmierne albo ewidentnie nieuzasadnione.

Prawodawca ma na myśli w szczególności sytuacje, gdzie żądania jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.

Zgodnie z RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo

- b) odmówić podjęcia działań w związku z żądaniem.

Po uzyskaniu informacji o wniesieniu opłaty, następuje realizacja wniosku i poinformowanie o spełnieniu żądania.

Z RODO... Artykuł 17. Prawo do usunięcia danych („prawo do bycia zapomnianym”).

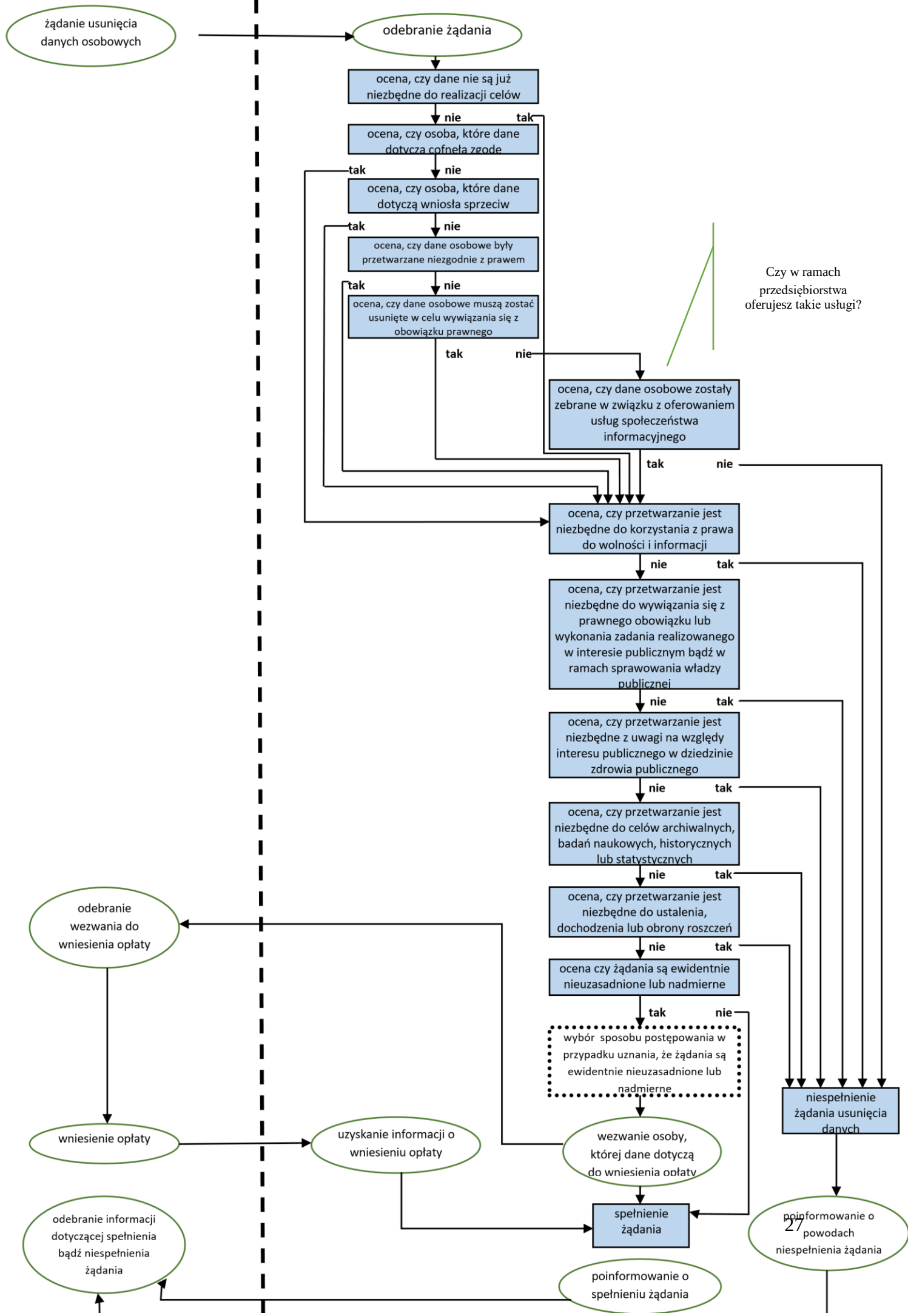
1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;*
- b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;*
- c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;*
- d) dane osobowe były przetwarzane niezgodnie z prawem;*
- e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;*
- f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.*

2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

- a) do korzystania z prawa do wolności wypowiedzi i informacji;*
- b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;*
- c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;*
- d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub*
- e) do ustalenia, dochodzenia lub obrony roszczeń.*



Czy w ramach przedsiębiorstwa oferujesz takie usługi?

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją. Po odebraniu takiego żądania, administrator ocenia, czy uprawnienie do wniesienia sprzeciwu zostało wyłączone na mocy przepisów szczególnych. Jeśli tak – nie trzeba spełniać żądania.

Jeśli jednak nie, to w dalszej kolejności należy ocenić, czy przetwarzanie danych jest niezbędne do wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Jeśli tak, to należy się zastanowić, czy pomimo sprzeciwu dane powinny być nadal przetwarzane. W przypadku odpowiedzi twierdzącej, nie musimy spełniać żądania. Jeśli jednak nie jest to niezbędne, należy ocenić, czy żądania są ewidentnie nieuzasadnione lub nadmierne.

Prawodawca ma na myśli w szczególności sytuacje, gdzie żądania jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.

Zgodnie z RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo
- b) odmówić podjęcia działań w związku z żądaniem.

Jeśli żądania nie są nadmierne ani nieuzasadnione albo jeśli są, a została wniesiona odpowiednia opłata, następuje uwzględnienie sprzeciwu (zaprzestanie przetwarzania danych w celu objętym sprzeciwem).

Inna sytuacja będzie miała miejsce, jeśli ocenimy, że przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów administratora lub strony trzeciej. W takim wypadku należy zadać pytanie, czy dane są przetwarzane na potrzeby marketingu bezpośredniego. Jeśli tak – oceniamy, czy żądania są ewidentnie nieuzasadnione lub nadmierne i postępujemy zgodnie z powyższą instrukcją, jeśli nie – oceniamy, czy pomimo sprzeciwu dane powinny być nadal przetwarzane i postępujemy analogicznie do wcześniej wskazanych sytuacji.

Z RODO...

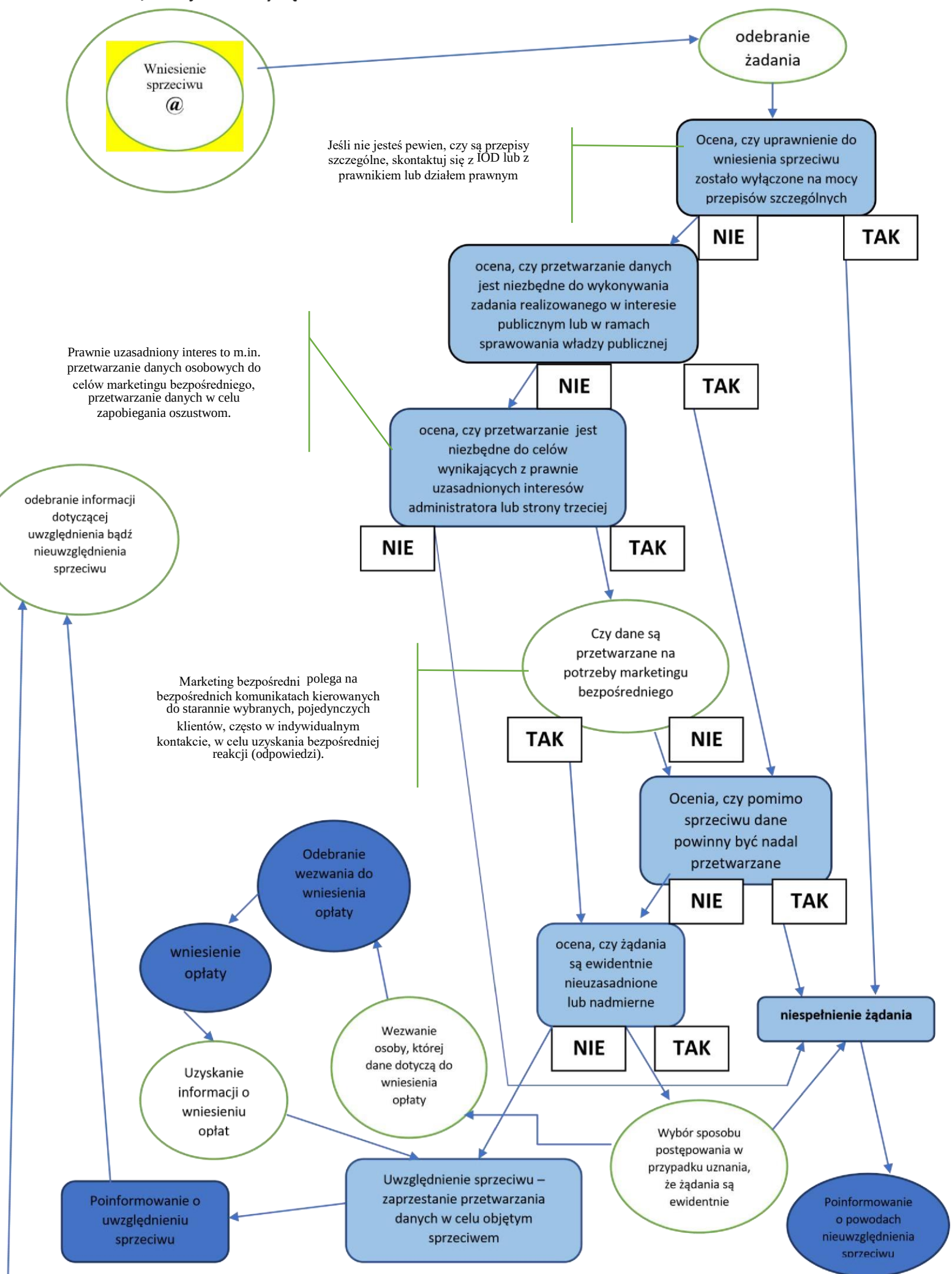
Artykuł 21. Prawo do sprzeciwu.

1. *Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.*
2. *Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.*

3. *Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.*
4. *Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.*
5. *W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.*
6. *Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.*

osoba, której dane dotyczą

administrator



XII. WNIOSEK OSOBY, KTÓREJ DANE DOTYCZĄ O PRZENIESIENIE DANYCH OSOBOWYCH

Osoba, której dane dotyczą, może złożyć wniosek o przeniesienie danych osobowych. W pierwszej kolejności administrator sprawdza, czy prawo do przenoszenia danych nie zostało wyłączone na mocy przepisów szczególnych. Jeśli nie zostało to należy ocenić, czy przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą.

Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

Jeśli przetwarzanie nie odbywa się na podstawie zgody, to w dalszej kolejności należy ocenić, czy przetwarzanie odbywa się w sposób zautomatyzowany.

Procesy zautomatyzowanego przetwarzania danych to procesy przetwarzania danych przy użyciu wyłącznie narzędzi informatycznych lub sztucznej inteligencji, mimo lub wbrew woli i bez intencji podmiotu, który jest nieświadomy ich występowania.

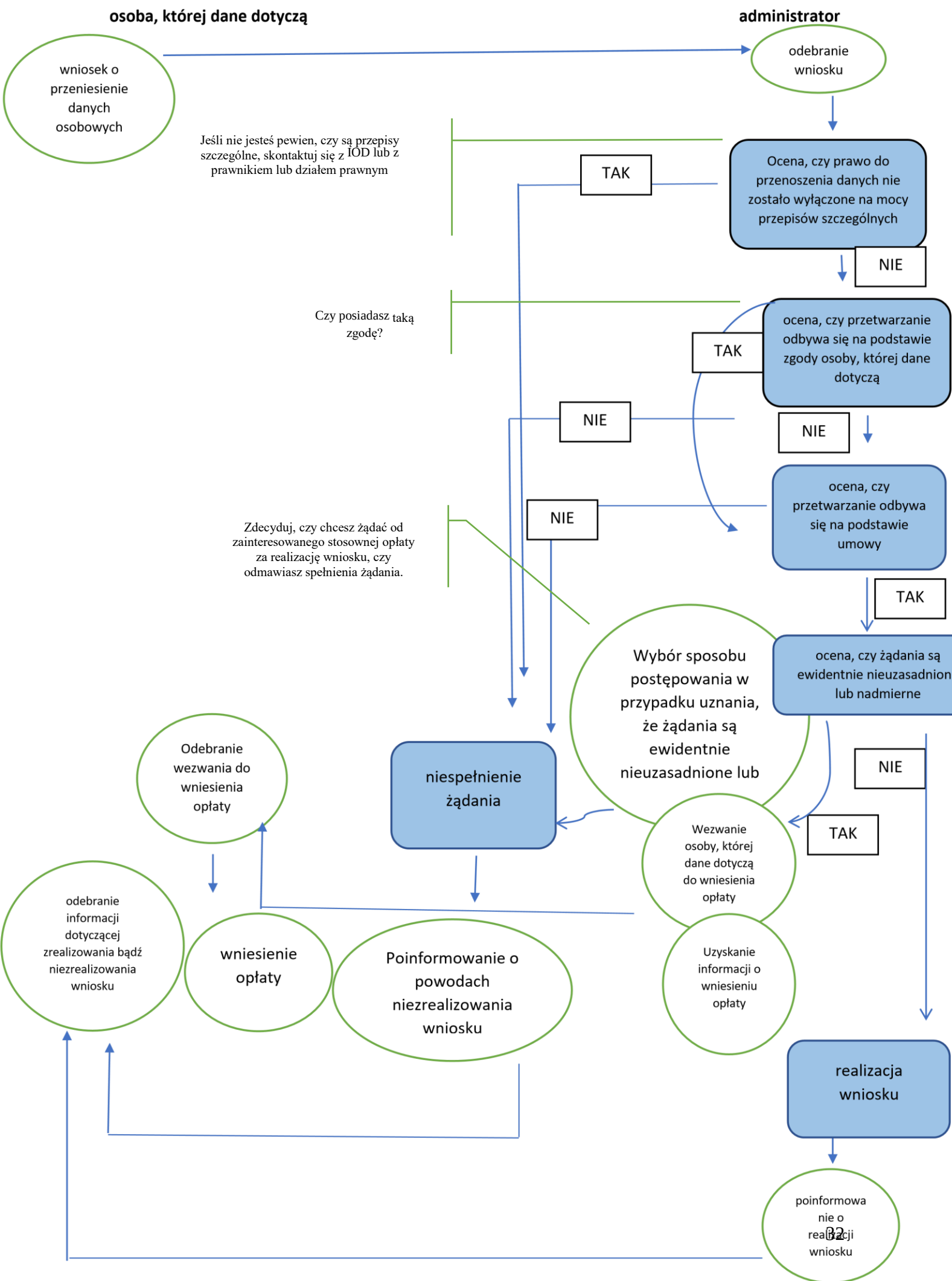
Jeżeli przetwarzanie odbywa się w sposób zautomatyzowany, należy ocenić, czy żądania są ewidentnie nieuzasadnione lub nadmierne. Jeśli nie są, to żądanie należy zrealizować.

Prawodawca ma na myśli w szczególności sytuacje, gdzie żądania jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.

Zgodnie z RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo
- b) odmówić podjęcia działań w związku z żądaniem.

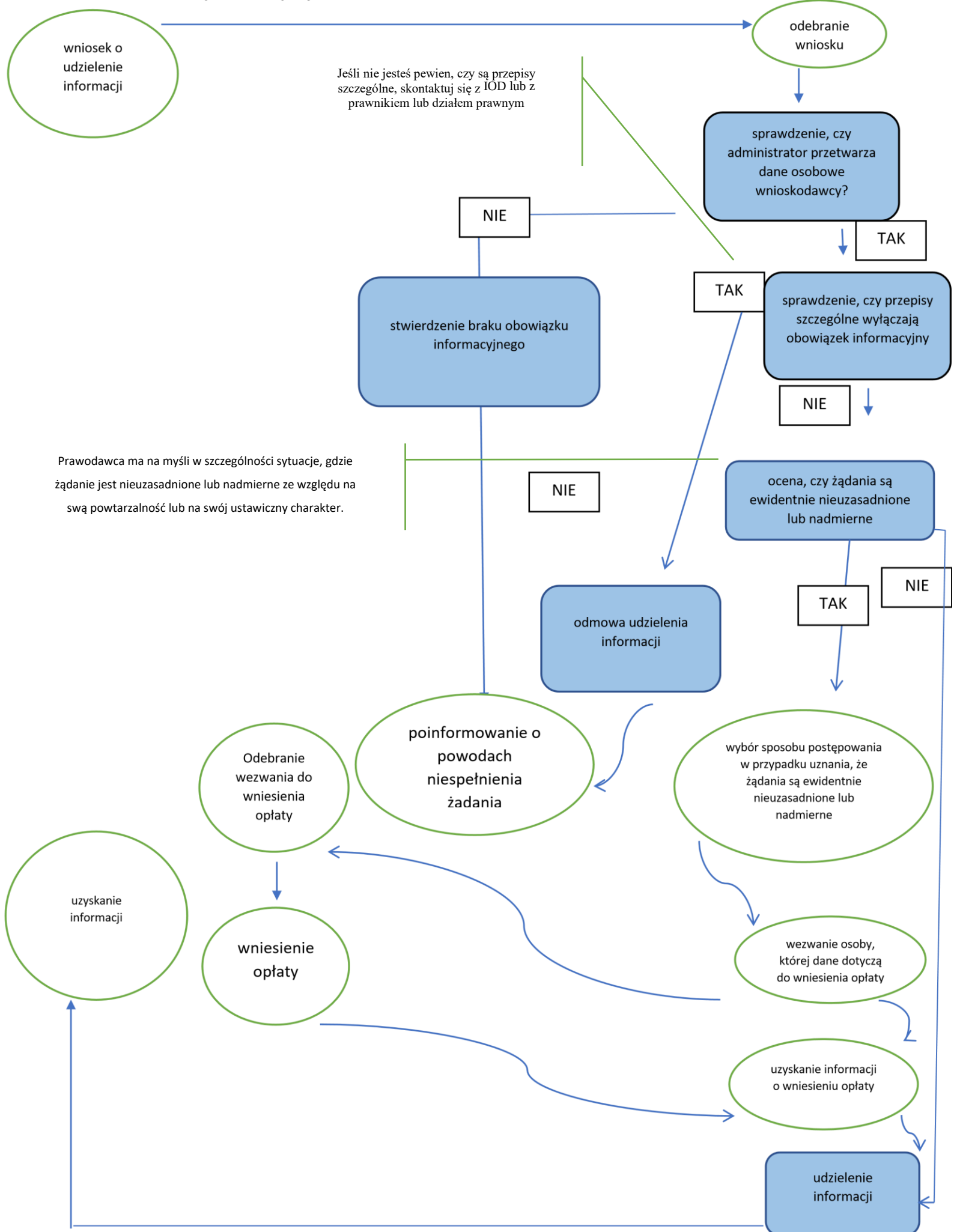
Po uzyskaniu informacji o wniesieniu opłaty, następuje realizacja wniosku i poinformowanie o realizacji wniosku.



XIII. WNIOSEK OD OSOBY, KTÓREJ DANE DOTYCZĄ O UDZIELENIE INFORMACJI

osoba, której dane dotyczą

administrator



Osoba, której dane dotyczą, może złożyć wniosek o udzielenie informacji o danych osobowych. Po odebraniu wniosku, administrator w pierwszej kolejności sprawdza, czy przetwarza dane osobowe konkretnej osoby. W tym miejscu należy przypomnieć, że przetwarzaniem danych osobowych jest też ich posiadanie. Jeśli nie – stwierdzamy brak obowiązku informacyjnego i informujemy osobę zainteresowaną o powodach niespełnienia żądania.

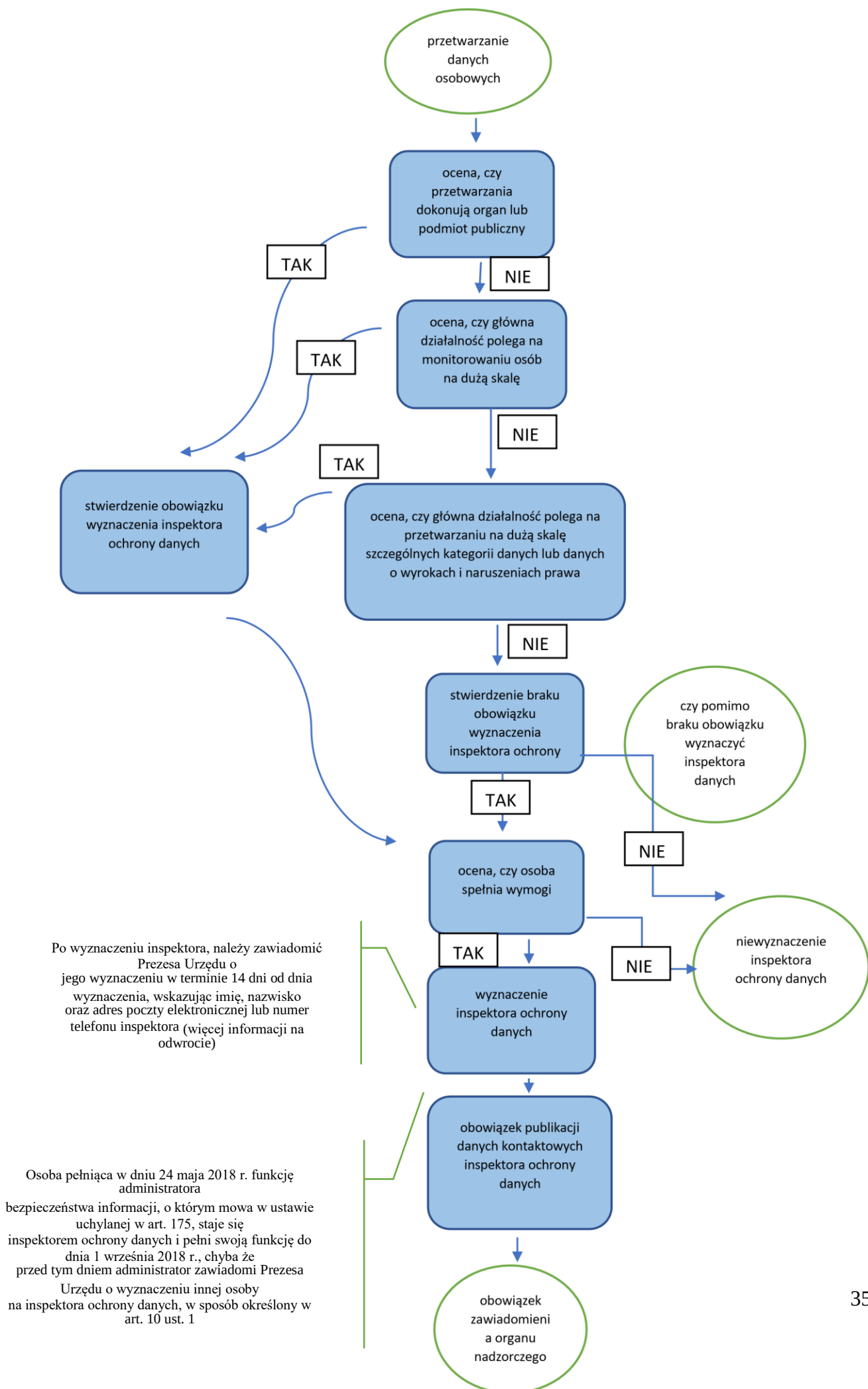
Jeśli jednak administrator posiada żądane dane osobowe, należy ustalić, czy przepisy szczególne wyłączają obowiązek informacyjny. Jeśli wyłączają, administrator może odmówić udzielenia informacji, informując jednocześnie o powodach jej nieudzielenia. Jeśli nie ma takich przepisów, należy ocenić, czy żądania są ewidentnie nieuzasadnione lub nadmierne.

Prawodawca ma na myśli w szczególności sytuacje, gdzie żądania jest nieuzasadnione lub nadmierne ze względu na swą powtarzalność lub na swój ustawiczny charakter.

Zgodnie z RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo
- b) odmówić podjęcia działań w związku z żądaniem.

Po uzyskaniu informacji o wniesieniu opłaty, następuje realizacja wniosku i udzielenie informacji.



Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

- a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
- c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Szczególne kategorie danych

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Jeżeli nie występuje żadna sytuacja z powyższych, nie ma obowiązku wyznaczania inspektora ochrony danych osobowych. Jeśli jednak występuje, należy stwierdzić powstanie **obowiązku wyznaczenia inspektora ochrony danych**.

Inspektor ochrony danych musi spełniać odpowiednie wymogi- jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.

Artykuł 39. Zadania inspektora ochrony danych.

1. Inspektor ochrony danych ma następujące zadania:

- a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- d) współpraca z organem nadzorczym;
- e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Po wyznaczeniu inspektora ochrony danych osobowych, powstaje także obowiązek publikacji danych kontaktowych inspektora ochrony danych oraz zawiadomienia organu nadzorczego.

Art. 10.

1. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie **14 dni** od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. 6
2. Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, o którym mowa w ust. 1. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej.
3. W zawiadomieniu oprócz danych, o których mowa w ust. 1, wskazuje się:
 - 1) imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna;
 - 2) firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą;
 - 3) pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 i 2;
 - 4) numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.
4. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.
5. W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorców, każdy z tych podmiotów dokonuje zawiadomienia, o którym mowa w ust. 1 i 4.
6. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Art. 11.

Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.