

Szkolenie ODO:

Przetwarzanie danych szczególnych kategorii, zautomatyzowane podejmowanie decyzji i udostępnianie danych

Szanowni Państwo,

szkolenie to ma na celu przybliżenie Państwu podstawowych zagadnień związanych z przetwarzaniem szczególnych kategorii danych osobowych, zautomatyzowanego podejmowania decyzji oraz udostępniania danych osobowych.

Tematyka przetwarzania danych osobowych szczególnych kategorii stanowi kontynuację w odniesieniu do omówionych już we wcześniejszych szkoleniach podstaw przetwarzania danych zwykłych, o których mowa w art. 6 RODO.

Wchodząca w roku 2021 r. ustawa o doręczeniach elektronicznych otwiera nowe możliwości zorganizowania pracy jednostek samorządu terytorialnego, w szczególności urzędów. Oznacza to jednak również nowe wyzwania z zakresu organizacji nowego procesu przetwarzania i wdrożenia nowych narzędzi służących do jego obsługi. Zagadnienie to wiąże się w szczególności z pojęciem zautomatyzowanego przetwarzania danych, w tym zautomatyzowanego podejmowania decyzji, ale wprowadzanie takich rozwiązań wiąże się również z innymi obszarami ochrony danych osobowych, jak choćby przeprowadzenie analizy ryzyka dla nowej czynności przetwarzania i podjęcie przez Administratora adekwatnych do wyników tej analizy działań.

Udostępnianie danych stanowi jedną z czynności przetwarzania, która z pewnością zasługuje na szersze omówienie w odniesieniu do zadań jednostek samorządu terytorialnego, którego jest nieodłączną częścią. Dowiedzą się Państwo między innymi na jakich podstawach mogą zostać udostępnione dane, a także w jaki sposób można zorganizować prawidłowe udostępnienie danych.

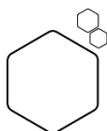
Szkolenie zakończone jest testem jednokrotnego wyboru.

Życzymy przyjemnej lektury!

Zespół Inspektora Ochrony Danych

Zestawienie tematów szkolenia:

Przetwarzanie szczególnych kategorii danych osobowych	3
Wyjątek nr 1 [art. 9 ust. 2 lit. a RODO]	4
Wyjątek nr 2 [art. 9 ust. 2 lit. b RODO]	4
Wyjątek nr 3 [art. 9 ust. 2 lit. c RODO]	5
Wyjątek nr 4 [art. 9 ust. 2 lit. d RODO]	5
Wyjątek nr 5 [art. 9 ust. 2 lit. e RODO]	6
Wyjątek nr 6 [art. 9 ust. 2 lit. f RODO]	6
Wyjątek nr 7 [art. 9 ust. 2 lit. g RODO]	6
Wyjątek nr 8 [art. 9 ust. 2 lit. h RODO]	6
Wyjątek nr 9 [art. 9 ust. 2 lit. i RODO]	7
Wyjątek nr 10 [art. 9 ust. 2 lit. j RODO]	7
Zautomatyzowane podejmowanie decyzji i profilowanie	8
Zautomatyzowane podejmowanie decyzji	8
Profilowanie	9
Zasada ogólna	9
Wyjątki od zasady	9
Decyzja oparta o zautomatyzowane przetwarzanie jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem	9
Decyzja oparta o zautomatyzowane przetwarzanie jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą	9
Decyzja oparta o zautomatyzowane przetwarzanie wydawana jest na podstawie wyraźnej zgody osoby, której dane dotyczą	10
Udostępnianie danych osobowych	11
Podstawy udostępnienia danych	11
Sposoby weryfikacji osoby chcącej uzyskać dane	11
Przekazanie danych	12
Podsumowanie	13



Przetwarzanie szczególnych kategorii danych osobowych

Przetwarzanie danych osobowych i podstawy na jakich się ono odbywa należą do podstawowych zagadnień ochrony danych. Są one również kluczowym elementem systemu ochrony danych każdego administratora. Wielokrotnie poruszany był już temat podstaw przetwarzania danych zwykłych, które uregulowane zostały w art. 6 RODO. Dla krótkiego przypomnienia, mowa oczywiście o przetwarzaniu:

1. na podstawie **zgody** wyrażonej przez osobę, której dane dotyczą (art. 6 ust. 1 lit. a),
2. w celu **zawarcia lub realizacji umowy**, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. b),
3. w ramach **obowiązku prawnego** ciążącego na administratorze (art. 6 ust. 1 lit. c),
4. na podstawie **żywothnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d),
5. niezbędnym do wykonania **zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej** powierzonej administratorowi (art. 6 ust. 1 lit. e),
6. niezbędnym do celów wynikających z **prawnie uzasadnionych interesów** (art. 6 ust. 1 lit. f),

z czego ostatnia przesłanka ma ograniczone zastosowanie w przypadku podmiotów publicznych.

W ramach codziennych zadań spotykają się Państwo również z danymi **szczególnych kategorii**, które zostały określone przepisem art. 9 ust. 1 RODO, wcześniej znane jako dane wrażliwe z nieobowiązującej już ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

O ile pierwszym problemem jest wciąż przede wszystkim identyfikacja danych osobowych, a więc rozpoznanie, które dane mogą prowadzić do identyfikacji osoby fizycznej, o tyle drugim wyzwaniem jest rozpoznanie danych szczególnych kategorii. Nie ma raczej wątpliwości co do tego, że do takich danych należy zaliczyć dane dotyczące zdrowia, o których jeszcze za chwilę. A jaką daną jest numer PESEL? Wydaje się, że pomimo zawierania w sobie wielu informacji o osobie fizycznej, które szczególnie w powiązaniu z innymi danymi, np. imieniem i nazwiskiem mogłyby stanowić źródło dokładnej identyfikacji tej osoby, numer PESEL należy traktować jako daną zwykłą.

No dobrze, **jakie więc dane są danymi wrażliwymi**? Zgodnie z brzmieniem przepisu art. 9 ust. 1 RODO są to:

- **dane osobowe ujawniające pochodzenie rasowe lub etniczne,**
- **poglądy polityczne,**
- **przekonania religijne lub światopoglądowe,**
- **przynależność do związków zawodowych,**
- **dane genetyczne,**
- **dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej,**
- **dane dotyczące zdrowia** (a nie jak w ustawie o ochronie danych osobowych z 1997 r. „*dane dotyczące stanu zdrowia*”),
- **dane dotyczące seksualności lub orientacji seksualnej.**

Należy w tym miejscu zaznaczyć, że [przetwarzanie tych danych jest co do zasady zabronione!](#) Odwrotnie więc do podstaw przetwarzania z art. 6 RODO, [podstawy przetwarzania z art. 9 ust. 2 RODO](#) stanowią jedynie wyjątki od reguły, które uprawniają do przetwarzania danych szczególnych kategorii.



Art. 9 ust. 1 RODO

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.

Skoro już wiadomo, jakie dane należą do zbioru danych szczególnych kategorii, może kilka przykładów. [Poglądami politycznymi mogą być poglądy wyrażane w czasie wyborów, czy protestów.](#) W podobny sposób można ujawniać swoje [przekonania religijne i światopoglądowe, uczestnicząc w obrzędach czy celebrując święta.](#) Dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, to na [przykład kontrola dostępu do laptopa przy wykorzystaniu odcisku palca lub inne zabezpieczenia badające choćby soczewkę oka.](#) Danymi dotyczącymi zdrowia będą natomiast nie tylko dane, z których można uzyskać informacje o stanie zdrowia, ale [również dane, na podstawie których można ustalić przynależność do danej przychodni.](#)

Jak już wspomniano, z uwagi na szczególny charakter, przetwarzanie tych danych jest co do zasady zabronione. Jest jednak od tej zasady niemało wyjątków.

Wyjątek nr 1 [art. 9 ust. 2 lit. a RODO]

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 art. 9 ust. 1 RODO.

Regulacja zawarta w art. 9 ust. 2 lit. a RODO i dotyczy zgody na przetwarzanie danych z art. 9 ust. 1 lit. a RODO. I ponownie, jak ma to miejsce w odniesieniu do danych zwykłych i art. 6 RODO, pomimo pierwszego miejsca spośród wskazanych w RODO przesłanek przetwarzania, w wymiarze funkcjonalnym zgoda – jakkolwiek będąca równorzędną podstawą przetwarzania – powinna być rozważana po pozostałych. Jest tak dlatego, że [tak samo jak zgoda z art. 6 ust. 1 lit. a RODO, zgoda z art. 9 ust. 2 lit. a RODO może zostać wycofana w dowolnym momencie.](#)

Wyjątek nr 2 [art. 9 ust. 2 lit. b RODO]

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.

Chodzi w szczególności o przetwarzanie danych wrażliwych w sprawach kadrowych, związanych z zatrudnieniem osób fizycznych. Należy pamiętać, że przesłanka ta dotyczy nie tylko osób zatrudnionych na podstawie umowy o pracę, ale również zleceniobiorców, w zakresie jaki jest niezbędny do realizowania obowiązków administratora. Przywołana przesłanka znajdzie zastosowanie również w obszarach ubezpieczeń społecznych, zabezpieczeń społecznych i pomocy społecznej, stąd znaleźć może szerokie zastosowanie w ośrodkach pomocy społecznej. Ostatnią – i wydaje się, że najszerszą – przesłanką jest ochrona socjalna, która mieści w sobie takie obszary jak ochrona zdrowia i bezpieczeństwo socjalne osób fizycznych. Jako przykład przetwarzania danych osobowych w powyższym zakresie może posłużyć przetwarzanie przez pracodawcę danych dotyczących chorób zawodowych pracownika; przetwarzanie danych o zdrowiu członków rodziny pracownika na potrzeby przyznania świadczeń socjalnych czy też przetwarzanie danych na potrzeby odprowadzania składek na ubezpieczenie społeczne.

Wyjątek nr 3 [art. 9 ust. 2 lit. c RODO]

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.

Przesłanka ta, która podobnie do zgody stanowi odbicie regulacji z art. 6 RODO, w tym przypadku art. 6 ust. 1 lit. d RODO, stanowi o przetwarzaniu danych wrażliwych, gdy jest to niezbędne dla ochrony żywotnych interesów. Wydaje się, że żywotnym interesem osób fizycznych będzie przede wszystkim ochrona ich życia i zdrowia, przyjmuje się jednak do tego katalogu również sprawy majątkowe. Odnosząc się natomiast do zdolności wyrażenia zgody – co wskazuje na pierwszeństwo tej przesłanki – należy ją rozumieć jako zdolność z jednej strony fizyczną, a więc możliwość złożenia oświadczenia w praktyce (przeszkodą może być stan zagrożenia życia, zdrowia, itp.), z drugiej zaś prawną, a więc brak zdolności prawnej do złożenia takiego oświadczenia (z taką sytuacją możemy spotkać się w przypadku dzieci lub osób ubezwłasnowolnionych).

Wyjątek nr 4 [art. 9 ust. 2 lit. d RODO]

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.

Przepis ten dotyczy działalności non profit, prowadzonych przez podmioty takie jak fundacje, stowarzyszenia, kościoły, itp. nie znajdzie więc co do zasady zastosowania w przypadku podmiotów publicznych, jakimi są jednostki samorządu terytorialnego.

Wyjątek nr 5 [art. 9 ust. 2 lit. e RODO]

Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

Dane szczególnych kategorii mogą być przetwarzane, jeżeli osoba fizyczna, której one dotyczą sama je upublicznia. Przez upublicznienie w sposób oczywisty rozumieć należy przede wszystkim wykorzystanie do tego celu środków masowego przekazu. Wydaje się więc, że jeżeli sama osoba fizyczna podała dane do publicznej wiadomości, to mogą być one w tym zakresie swobodnie przetwarzane.

Wyjątek nr 6 [art. 9 ust. 2 lit. f RODO]

Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy.

Jak wskazuje motyw 52, przesłanka ta dotyczy przetwarzania danych wrażliwych w ramach postępowań sądowych, administracyjnych lub innych postępowaniach pozasądowych. Uprawnia do przetwarzania takich danych również sądy, niezależnie od tego jakimi sprawami się one zajmują. Znajdzie więc zastosowanie do działań sądów cywilnych, karnych, administracyjnych, ale również do sądów polubownych. Przesłanka ta dotyczy również działań stron i ich obrońców lub pełnomocników podejmowanych w ramach tych postępowań.

Wyjątek nr 7 [art. 9 ust. 2 lit. g RODO]

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.

Pojęcie ważnego interesu publicznego nie zostało zdefiniowane w RODO, wydaje się jednak, że chodzi w szczególności o takie obszary jak zabezpieczenie społeczne czy zdrowie. Drugą przesłanką jest tu istnienie przepisu obowiązującego prawa unijnego lub krajowego, który pozwala na dane działanie. Spełniony musi być jednocześnie warunek proporcjonalności do wyznaczonego celu, a więc przyjęte rozwiązania nie powinny wykraczać poza ten cel, jak również nie mogą naruszać prawa do ochrony danych osobowych, przewidując odpowiednie i konkretne środki ochrony praw podstawowych i interesów osób fizycznych. Oznacza to, że regulacje powinny obejmować sposób zabezpieczenia przetwarzania, aby zminimalizować ryzyko wystąpienia nieprawidłowości i ich potencjalne negatywne skutki dla osób fizycznych. Jako przykład posłużyć może przetwarzanie danych szczególnych kategorii w celu organizacji zajęć dla uczniów z orzeczeniem o potrzebie kształcenia specjalnego czy zapewnienia mu wsparcia psychologiczno-pedagogicznego.

Wyjątek nr 8 [art. 9 ust. 2 lit. h RODO]

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 art. 9 ust. 3 RODO.

Regulacja ta obejmuje kwestie związane z ochroną zdrowia, w tym powiązane z kadrami zagadnienia medycyny pracy i oceny zdolności pracownika do pracy, w tym prowadzenie badań wstępnych, okresowych pracownika. Przede wszystkim jednak chodzi o ochronę zdrowia i działających w jej ramach lekarzy, dentystów, fizjoterapeutów, pielęgniarek i pozostałego personelu medycznego. Należy zaznaczyć, że osoby te są zobowiązane do zachowania w poufności informacji dotyczących pacjentów.

Wyjątek nr 9 [art. 9 ust. 2 lit. i RODO]

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.

Przyjąć należy, że przetwarzanie w tym zakresie dotyczy spraw związanych z zachowaniem zdrowia publicznego, a więc przede wszystkim profilaktykę zdrowotną, promowanie zdrowia i edukowanie w tym zakresie, jak również przeciwdziałanie i zapobieganie zagrożeniom zdrowotnym, takim jak epidemia SARS-CoV-2. Tak jak we wcześniejszych przypadkach, również tu należy mieć na względzie ochronę praw i wolności osób fizycznych, jak również podstawą do działań powinny być przepisy obowiązującego prawa unijnego lub krajowego.

Wyjątek nr 10 [art. 9 ust. 2 lit. j RODO]

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.

Tak jak w poprzednich przypadkach również tutaj podstawą powinny być przepisy obowiązującego prawa unijnego lub krajowego, które uwzględniają stosowne środki ochrony i nie naruszają istoty prawa do ochrony danych. Celem przetwarzania jest gromadzenie materiałów do zadań archiwalnych, do badań naukowych lub historycznych, a także celów statystycznych. Jest to więc szeroki katalog działań podejmowanych przez podmioty – nie tylko państwowe – zajmujące się badaniami historycznymi i statystycznymi.

Zautomatyzowane podejmowanie decyzji i profilowanie

Kolejnym istotnym tematem, szczególnie w odniesieniu do zmian w Kodeksie postępowania administracyjnego i innych ustaw sektorowych, wchodzących w życie w 2021 r. wraz z ustawą z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, jest [zautomatyzowane podejmowanie decyzji](#).

Z pojęciem tym spotykamy się w przepisie art. 22 RODO, gdzie mowa o [prawie osoby fizycznej do niepodlegania wyłącznie zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu](#).



Artykuł 22 RODO

1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:
 - a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
 - b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
 - c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.
4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Zautomatyzowane podejmowanie decyzji

Na początek dla przypomnienia, czym jest zautomatyzowane przetwarzanie? Wprawdzie RODO nie definiuje tego pojęcia, jednak wydaje się, że [zautomatyzowanym przetwarzaniem będzie każde działanie na danych osobowych, które odbywa się bez ingerencji człowieka](#). Decyzją opierającą się wyłącznie na zautomatyzowanym przetwarzaniu będzie więc taka, która podejmowana jest całkowicie bez udziału człowieka, a więc na przykład przez [system obliczający punktację na podstawie udostępnionego formularza](#). Decyzją taką może być wyliczenie wysokości opłaty za wywóz odpadów, jeżeli system wylicza ją automatycznie, a urzędnik jedynie potwierdza tę decyzję. Innym przykładem może być rekrutacja do placówek oświatowych, gdzie system decyduje o losie kandydata na podstawie kryteriów w uzupełnionym formularzu. Tego typu decyzje wywołują skutki prawne lub wpływają na osobę, której one dotyczą w podobny sposób.

Profilowanie

Profilowanie nie musi być powiązane ze zautomatyzowanym przetwarzaniem i co do zasady nie znajdzie zastosowania w jednostkach samorządu terytorialnego. **Profilowaniem określa się takie działanie, które na podstawie uzyskanych danych kreuje profil (w rozumieniu modelu zachowań, cech osobowości, itp.) osoby fizycznej.** Pozyskiwane dane mogą mieć szeroki zakres, od danych podstawowych do danych szczególnych kategorii, takich jak dane dotyczące zdrowia, światopoglądu, jak również lokalizacji, nawyków. Profilowanie kojarzone jest szerzej w kontekście mediów społecznościowych, które na podstawie pozyskanych informacji kreują profile tych osób, przewidując ich przyszłe zachowania, które to predykcje stanowią istotny czynnik sprzedażowy dla reklamodawców, umożliwiając dopasowanie reklamy do osoby, która z dużą dozą prawdopodobieństwa będzie nią zainteresowana.

Zasada ogólna

Ogólną zasadą wyrażoną w RODO jest **prawo osoby fizycznej do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu.** Oznacza to, że jest ono dozwolone, jednak powinno być nadzorowane i ostatecznie potwierdzone przez człowieka. Należy zaznaczyć, że chodzi tu o realny udział człowieka w podjęciu decyzji, a nie jedynie podpisanie wydruku z systemu.

W każdym przypadku podejmowania decyzji w oparciu o zautomatyzowane przetwarzanie, powinno więc ono podlegać kontroli prawidłowości rozstrzygnięcia przez człowieka, jak również zapewnione powinno być prawo do rozpatrzenia odwołania od takiej decyzji przez człowieka.

Wyjątki od zasady

Od opisanej wyżej zasady zostały przewidziane trzy wyjątki:

Decyzja oparta o zautomatyzowane przetwarzanie jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem.



Przesłanka ta znajdzie zastosowanie w sytuacji, gdy zautomatyzowane podjęcie decyzji stanowi warunek konieczny do zawarcia umowy pomiędzy osobą, której dane dotyczą, a administratorem. Z uwagi na charakter zawieranych przez jednostki samorządu terytorialnego umów wydaje się, że przesłanka ta nie znajdzie zastosowania.

Decyzja oparta o zautomatyzowane przetwarzanie jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.



Najistotniejsza z punktu widzenia jednostek samorządu terytorialnego przesłanka, w szczególności w kontekście przepisów ustawy o doręczeniach elektronicznych, która w dużej mierze umożliwi takie podejmowanie decyzji. Zmiany obejmują na przykład możliwość udzielania automatycznych odpowiedzi bez udziału czynnika ludzkiego. Należy jednak zaznaczyć, że aby móc legalnie skorzystać z tej przesłanki ustawodawca powinien przewidzieć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Przepisy ustawy o doręczeniach elektronicznych takich środków na chwilę obecną nie przewidują. Brak ujęcia takich środków przez ustawodawcę powoduje problem, ponieważ przesłanka nie zostaje wyczerpana, a w konsekwencji nie powinna być ona zastosowana.

*Ważna informacja

Przywołana ustawa obejmuje między innymi zmianę przepisów Kodeksu postępowania administracyjnego, ustawy o utrzymaniu czystości i porządku w gminach, Ordynacji podatkowej, Prawa o postępowaniu przed sądami administracyjnymi, ustawy o zmianie imienia i nazwiska, ustawy o dowodach osobistych, Prawa o aktach stanu cywilnego, czy Prawa zamówień publicznych.

Decyzja oparta o zautomatyzowane przetwarzanie wydawana jest na podstawie wyraźnej zgody osoby, której dane dotyczą.



Przesłanka ta stanowi o możliwości zautomatyzowanego przetwarzania w celu wydania decyzji w przypadku uzyskania wyraźnej zgody osoby, której dane dotyczą. Wydaje się, że również ona nie znajdzie szerokiego zastosowania w jednostkach samorządu terytorialnego.

Zarówno w przypadku pierwszej, jak i trzeciej omawianej przesłanki, to administrator odpowiada za wdrożenie środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Środki te powinny przewidywać co najmniej prawo do wyrażenia własnego stanowiska i zakwestionowania decyzji przez osobę, której dane dotyczą, a także umożliwienie rozpatrzenia takiego odwołania przez człowieka.

Zaznaczyć należy również surowe ograniczenie przetwarzania w odniesieniu do danych szczególnych kategorii. Tak jak w przypadku opisanych wyjątków, powinny zostać przewidziane środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Ponadto, **zautomatyzowane podejmowanie decyzji nie może opierać się na danych szczególnych kategorii, chyba że osoba, której dane dotyczą wyrazi na to wyraźną zgodę lub przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym**, przy zachowaniu wszelkich gwarancji, o których mowa w art. 9 ust. 2 lit. g RODO.

Udostępnianie danych osobowych

Podstawy udostępnienia danych

Udostępnienie danych to jedna z czynności przetwarzania polegająca na przekazaniu danych innemu administratorowi. Jest to istotny element odróżniający udostępnienie od powierzenia przetwarzania danych. Z powierzeniem przetwarzania mamy do czynienia w sytuacji, gdy administrator przekazuje dane innemu podmiotowi, wskazując jednocześnie w jakich celach i w jaki sposób dane te mają być przetwarzane (np. księgowość, centrum usług wspólnych). **Udostępnienie danych natomiast wiąże się z przekazaniem danych przez jednego administratora drugiemu administratorowi, gdzie obaj przetwarzają te dane we własnych celach i co do zasady samodzielnie określając sposoby tego przetwarzania.** Przykładem udostępnienia jest choćby przekazanie Policji fragmentu nagrania z monitoringu wizyjnego, udostępnienie danych z ewidencji PESEL, przekazanie danych niezbędnych do przeprowadzenia postępowania między jednostkami samorządu terytorialnego, np. między ośrodkami pomocy społecznej lub między ośrodkiem pomocy społecznej a szkołą.

Podstawą udostępnienia może być:

- **przepis obowiązującego prawa,**
- **niezbędność do realizacji prawnie uzasadnionych interesów administratora,**
- **wyraźna zgoda osoby, której dotyczy udostępnienia.**

Najważniejszą, bo najczęściej stosowaną w podmiotach publicznych podstawą, będzie **istnienie przepisów obowiązującego prawa, krajowego lub unijnego, które uprawniają lub nakładają obowiązek udostępnienia danych.** Z sytuacją taką będziemy mieć styczność zarówno w przypadku, gdy przepisy wprost umożliwiają udostępnienie, jak choćby w przypadku przekazywania danych w związku z dożywianiem w szkołach, czy ustawy o ewidencji ludności.

Udostępnienie może się odbyć również na podstawie **wyraźniej zgody osoby, której ono dotyczy, a więc w sytuacjach, gdy wprawdzie nie istnieje przepis pozwalający na takie udostępnienie, ale osoba, której ono dotyczy wyraża zgodę na przekazanie danych lub wręcz sama o to wnosi.** RODO nie wskazuje sposobu odebrania zgody, wydaje się jednak, że wskazanym działaniem jest uzyskanie jej w formie utrwalonej, w celach dowodowych.

Wreszcie, udostępnienia można dokonać **w przypadku prawnie uzasadnionych interesów administratora, jednakże w takim przypadku należy wykazać, że są one ważniejsze niż interesy osoby, której ma dotyczyć udostępnienie.**

Sposoby weryfikacji osoby chcącej uzyskać dane

Pierwszym krokiem przy udostępnianiu danych powinna być **weryfikacja tożsamości podmiotu, który wnosi o to udostępnienie, a także ustalenie, czy jest on podmiotem uprawnionym do uzyskania informacji.** W przypadku udostępnienia na podstawie przepisów prawa, to właśnie w tym przepisach szukać należy, czy jest to podmiot uprawniony. Odnosząc się natomiast do weryfikacji tożsamości należy mieć na uwadze podjęcie takich działań, które z jednej strony zminimalizują ryzyko udostępnienia danych osobie nieuprawnionej, z drugiej zaś zabezpieczą prywatność tej osoby (np. nie zdradzając jej danych w trakcie pytań kontrolnych).

Sposoby weryfikacji tożsamości będą się oczywiście różnić w zależności od tego, w jakiej formie możliwe będzie jej przeprowadzenie. O ile więc naturalnym wydaje się ustalenie tożsamości na podstawie okazanego dowodu tożsamości przy fizycznej obecności tej osoby, tak przeprowadzenie prawidłowej i skutecznej weryfikacji na odległość może przysporzyć większych problemów.

Jednym z rozwiązań, jakie można zastosować np. przy kontaktowaniu się przez telefon, są [pytania kontrolne](#), a więc pytania o dane lub informacje, których nie powinna posiadać osoba nieuprawniona. Mogą to więc być pytania o dane tej osoby, jak choćby numer PESEL, jak również okoliczności dotyczące danego postępowania. [Należy pamiętać, aby weryfikacja taka była zorganizowana w sposób aktywny](#), tj. to osoba powinna udzielić odpowiedzi na pytanie, a nie jedynie potwierdzać wskazane dane. Przykładowo, pytanie powinno brzmieć „Jaki jest Pani/Pana numer PESEL?”, a nie „Czy numer PESEL 12345678901 jest Pani/Pana?”. Dodatkowo, w opisanym przypadku wskazane będzie zapytanie jedynie o część numeru PESEL, jeżeli będzie to wystarczające do skutecznej weryfikacji. Takie działanie zapobiegnie przekazaniu danych w przypadku, gdyby była to jednak osoba nieuprawniona.

Podobne zasady znajdą zastosowanie w przypadku innych pytań kontrolnych. [Ważne jest to, aby to osoba chcąca uzyskać dane odpowiadała na pytania otwarte tak, aby nie przekazać jej żadnych istotnych informacji, a jedynie uzyskać potwierdzenie ich posiadania przez tę osobę.](#)

W odniesieniu do kontaktu elektronicznego, a więc np. poczty elektronicznej, [należy zwracać uwagę na adres nadawcy, a w razie wątpliwości potwierdzać tożsamość osoby innymi kanałami](#), np. telefonicznie. Jeżeli natomiast mowa o spotkaniach przy wykorzystaniu komunikatorów, [należy zmierzać do przetwarzania jak najmniejszej ilości danych](#). Należy mieć na względzie, że okazanie dowodu tożsamości w sieci, również podczas transmisji czy połączenia na żywo, może zostać przechwycone, a w konsekwencji wykorzystane np. do zaciągnięcia na te dane pożyczki.

[Przekazanie danych](#)

Również to, w jaki sposób dane zostaną przekazane rodzi wyzwania organizacyjne, szczególnie w odniesieniu do formy elektronicznej.

W każdym przypadku [należy pamiętać o ewentualnej anonimizacji lub pseudonimizacji](#), jeżeli zakres danych podlegających udostępnieniu jest węższy niż dane zawarte przykładowo w dokumentacji podlegającej udostępnieniu.

W przypadku przesyłania danych drogą elektroniczną należy zabezpieczyć te dane, przynajmniej przez [opatrzenie pliku hasłem, które następnie powinno podlegać przekazaniu innym kanałem](#), np. telefonicznie. Przesłanie hasła do pliku nawet w odrębnej wiadomości, nie minimalizuje w wystarczającym stopniu ryzyka błędu. Wskazane jest również [szyfrowanie wiadomości](#). Działania takie minimalizują ryzyko zapoznania się z udostępnianymi treściami przez osoby nieuprawnione.

Warto jeszcze wspomnieć na koniec o wniosku, na podstawie którego udostępniane są dane. Wprawdzie brak jest ogólnej zasady, z jakich elementów powinien się składać, jednak [wydaje się, że podstawowy zakres wniosku powinien obejmować datę, oznaczenie podmiotu wnoszącego o udostępnienie oraz podmiotu, który ma go dokonać, wskazanie podstawy prawnej udostępnienia, jeżeli istnieje, podpisu osoby uprawnionej, a także innych okoliczności dotyczących udostępnienia, które będą się zmieniać w zależności od tego, jakich danych dotyczy udostępnienie. Wniosek taki, w celach dowodowych, powinien przyjąć utrwaloną formę \(pisemną lub elektroniczną\).](#)

Kończąc rozważania nad zagadnieniem udostępnienia danych **warto wspomnieć również o aspekcie ochrony danych osobowych dostępu do informacji publicznej**. Zgodnie z przepisem art. 5 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, **prawo dostępu do informacji publicznej jest ograniczone prywatnością osoby fizycznej**. Nie dotyczy ono informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji. **Osoby fizyczne, których dotyczą informacje, mogą również z tego ograniczenia zrezygnować**. W takim przypadku możliwe jest przekazanie informacji ich dotyczących, nie naruszając tym samym ich prywatności. Rozważając możliwość przekazania informacji publicznej należy mieć na względzie przede wszystkim, czy dana informacja stanowi informację publiczną, w jakim zakresie, czy narusza ona prywatność osoby fizycznej, a po ustaleniu tych okoliczności, zastanowić się nad ewentualną anonimizacją lub pseudonimizacją danych.

Podsumowanie

Przetwarzanie szczególnych kategorii stanowi codzienny element każdego podmiotu publicznego, dlatego **szczególnie ważne jest świadome i rozważne wykorzystywanie tych danych, nie tylko na poziomie całego systemu ochrony danych przyjętego przez administratora, ale również – a może nawet zwłaszcza – przez pracowników administratora**.

Postępująca cyfryzacja podmiotów publicznych przynosi wiele ułatwień, ale również i wyzwań, z którymi mierzą się administratorzy. **Ważne, aby nie zapominać w tym o ochronie prywatności osób fizycznych i dotyczących ich danych osobowych, wdrażając środki ochrony od najwcześniejszych etapów organizowania narzędzi i zasad takiego postępowania**. Szczególne miejsce zajmować będzie ochrona danych niewątpliwie w przypadku wprowadzania rozwiązań dopuszczonych na podstawie ustawy o doręczeniach elektronicznych.

Udostępnianie danych, stanowiące codzienność podmiotów publicznych, powinno być zorganizowane w sposób zapewniający **prywatność osób, których ono dotyczy, ochronę ich danych osobowych, a także umożliwiać rozliczalność administratora**.

