



**Stanowisko Amerykańskiej Izby Handlowej w Polsce (AmCham) dotyczące projektu Ustawy o ochronie danych osobowych z dnia 12 września 2017 roku („Projekt Ustawy”)**

*1. Wiek zgody - osoby poniżej 13 roku życia przebywające fizycznie w Polsce – art.*

*3 Projektu Ustawy*

**Rekomendacja: Artykuł 3 nie powinien zawierać postanowienia dotyczącego lokalizacji dziecka w wieku poniżej 13 lat.**

**Wyjaśnienie:**

Ogólne Rozporządzenie o Ochronie Danych („**Rozporządzenie**”) stanowi, że w odniesieniu do oferowania usług społeczeństwu informacyjnego bezpośrednio dziecku, przetwarzanie na podstawie zgody jest dokonywane zgodnie z prawem jeżeli dziecko ma co najmniej 16 lat. Jeżeli dziecko nie ukończyło 16 roku życia, przetwarzanie takie jest zgodne z prawem tylko wtedy i w takim zakresie, w jakim rodzic/opiekun prawny dziecka wyraził zgodę lub potwierdził jej wydanie. Państwa członkowskie mogą obniżyć limit wieku, jednakże nie może być on niższy niż 13 lat.

Zwracamy uwagę, że Rozporządzenie daje państwom członkowskim prawo jedynie do obniżenia granicy wieku. Rozporządzenie nie zawiera innego upoważnienia dla państw członkowskich niż obniżenie wieku zgody do 13 lat. Dotyczy to w szczególności wszelkich dodatkowych wymogów, takich jak fizyczna lokalizacja dziecka poniżej 13 roku życia, zawartych w Projekcie Ustawy. W związku z tym ten dodatkowy element nie wchodzi w zakres upoważnienia ustanowionego zgodnie z Rozporządzeniem i powinien zostać skreślony.

Ponadto artykuł 3 Rozporządzenia ustanawia zasadę terytorialności skupiając się na siedzibie jednostki organizacyjnej administratora danych lub podmiotu przetwarzającego a nie na lokalizacji obywateli. Ustawodawstwo państw członkowskich nie powinno być sprzeczne z tą zasadą. Zróżnicowane podejście państw członkowskich w tym zakresie mogłoby prowadzić do nieporozumień. Koncepcja jednostki organizacyjnej jest powszechnie akceptowana i pozwala międzynarodowym podmiotom unikać konieczności mierzenia się z ustawodawstwami wielu państw.

Ponadto uzasadnienie Projektu Ustawy nie wyjaśnia, dlaczego wymóg dotyczący lokalizacji miałby mieć zastosowanie do wszystkich dzieci poniżej 13 roku życia obecnych (nawet tymczasowo) w Polsce.

*2. Szczególne kategorie danych osobowych*

**Rekomendacja: Projekt Ustawy powinien uwzględniać możliwość przetwarzania danych dotyczących zdrowia, danych genetycznych i biometrycznych w celu realizacji umowy.**

**Wyjaśnienie:**

Definicja szczególnych kategorii danych osobowych zawarta w Rozporządzeniu jest bardzo szeroka, zawiera ona w sobie dane obejmujące pochodzenie etniczne lub rasowe, poglądy polityczne, poglądy religijne i filozoficzne, dane dotyczące seksualności lub orientacji seksualnej, przynależność do związków zawodowych oraz dane dotyczące zdrowia, dane genetyczne i biometryczne.

Artykuł 9 ust. 4 Rozporządzenia przewiduje możliwość wprowadzenia przez państwa członkowskie dalszych warunków, w tym ograniczeń, dotyczących przetwarzania danych genetycznych, biometrycznych oraz danych dotyczących zdrowia. Dla niektórych przedsiębiorców, przetwarzanie tego rodzaju danych może być nieodłącznym elementem prowadzonej działalności, w tym realizacji zobowiązań umownych. W takich przypadkach przetwarzanie danych wrażliwych może okazać się niezbędne.

### *3. Ograniczenia praw osób, których dane dotyczą*

**Rekomendacja: Projekt Ustawy powinien uwzględnić przewidzianą w Rozporządzeniu konieczność zachowania równowagi pomiędzy prawem do ochrony danych osobowych a innymi prawami i wolnościami, w tym prawem do prowadzenia działalności gospodarczej.**

**Wyjaśnienie:**

Motyw 4 Rozporządzenia jasno stwierdza, że prawo do ochrony danych osobowych nie jest prawem absolutnym. Musi ono zostać zrównoważone z innymi prawami i wolnościami, w tym z prawem do prowadzenia działalności gospodarczej. Projekt Ustawy powinien zawierać w sobie powyższe postanowienia zapewniające swobodę prowadzenia działalności gospodarczej.

### *4. Ograniczenie obowiązku informacyjnego*

**Rekomendacja: Projekt Ustawy powinien zapewnić, że wypełnienie obowiązku informacyjnego w przypadku pozyskiwania danych w inny sposób niż od osoby, której dane dotyczą może podlegać ograniczeniom w następujących sytuacjach:**

- jeżeli szkodziłoby to interesom administratora danych w zakresie własności intelektualnej i tajemnicy przedsiębiorstwa;
- jeżeli szkodziłoby to interesom strony trzeciej, włączając w to inną osobę, której dotyczą dane;
- jeżeli wymagałoby to od administratora danych zebrania dodatkowych danych odnoszących się do osoby, której te dane dotyczą;
- jeżeli uniemożliwiłoby to administratorowi danych spełnienie konkurencyjnego obowiązku prawnego, zawierającego w sobie obowiązek zachowania tajemnicy zawodowej.

### *5. Ograniczenie prawa do usunięcia danych*

Artykuł 17 ust. 3 pkt b Rozporządzenia przewiduje, że prawo do usunięcia danych nie ma zastosowania w zakresie w jakim przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub państwa członkowskiego, któremu podlega administrator.

**Rekomendacja: Projekt Ustawy oraz inne właściwe akty prawne powinny odzwierciedlać treść artykułu 17 ust. 3 pkt b Rozporządzenia i uwzględnić postanowienie umożliwiające administratorowi danych powstrzymanie się od usunięcia danych na żądanie osoby, której dane dotyczą, w sytuacji gdy może to być sprzeczne z innymi obowiązkami, w tym wynikającymi z przepisów prawa.**

### *6. Ograniczenie prawa dostępu*

Artykuł 23 ust. 1 pkt i Rozporządzenia pozwala na ograniczenie zakresu praw i obowiązków, jeżeli ograniczenie takie służy ochronie osoby, której dane dotyczą lub praw i wolności innych osób. Artykuł 15 ust. 4 Rozporządzenia stanowi, że prawo dostępu nie może niekorzystnie wpływać na prawa i wolności innych osób. Prawa i wolności innych osób obejmują prawa i wolności osób, których dane dotyczą, jak i administratorów (np. swoboda działalności gospodarczej).

**Wyjaśnienie: Projekt Ustawy powinien odpowiednio odzwierciedlać treść art. 23 ust. 1 pkt i) Rozporządzenia, poprzez wprowadzenie następujących ograniczeń prawa dostępu:**

- jeśli administrator danych nie może spełnić żądania bez ujawniania informacji dotyczących osoby trzeciej, która może być zidentyfikowana na ich podstawie, administrator nie powinien być zobowiązany do wykonania wniosku, chyba że osoba trzecia wyraziła zgodę na ujawnienie informacji osobie składającej wniosek.
- prawa własności intelektualnej powinny być chronione, a administratorzy nie powinni być zobowiązani do zapewnienia dostępu osobom, których dane dotyczą, jeśli przez to udostępnione zostaną informacje chronione prawem własności intelektualnej.
- jeśli dostarczenie takich informacji okaże się niemożliwe lub pociągałoby za sobą nieproporcjonalny wysiłek administratora danych. Istnieją pewne dane, które są przechowywane w taki sposób, że dostarczenie ich przez administratora osobom, których dane dotyczą, pociągałoby za sobą ogromne obciążenie finansowe oraz obciążenie zasobów, które nie byłoby współmierne z wartością danych dla osoby, której one dotyczą.

*7. Prawo do niepodlegania zautomatyzowanym decyzjom*

Artykuł 22 Rozporządzenia przewiduje, że 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.”

Jednakże artykuł 22 Rozporządzenia nie powinien być odczytywany jako zakaz wydawania decyzji, opartych wyłącznie na zautomatyzowanym przetwarzaniu (wywołujących wobec osoby, której dane dotyczą skutki prawne lub w podobny sposób istotnie na nią wpływających). Raczej powinien być traktowany jako możliwość dla osoby, której dane dotyczą do sprzeciwienia się takiej decyzji.

**Rekomendacja: Zdecydowanie sugerujemy, aby Projekt Ustawy zawierał w sobie wyłączenia przedstawione w art. 22 ust 2 pkt b Rozporządzenia oraz zezwolenie na decyzje, których mowa w art. 22 ust. 1 Rozporządzenia, gdy administrator danych opiera się na podstawie prawnej zawartej w art. 6 ust. 1 pkt a oraz pkt f Rozporządzenia. Takie podejmowanie decyzji powinno podlegać takim samym zabezpieczeniom jak te określone w art. 22 ust. 3 Rozporządzenia, mianowicie: „co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji”.**

*8. Prawo Prezesa Urzędu Ochrony Danych Osobowych („PUODO”) do ujawnienia informacji oznaczonych przez stronę jako tajemnica przedsiębiorstwa – art. 49 Projektu Ustawy*

**Rekomendacja: Usunięcie prawa PUODO do ujawnienia informacji oznaczonych przez stronę jako tajemnica przedsiębiorstwa.**

**Wyjaśnienie:**

Projekt Ustawy daje PUODO prawo do uchylenia – według własnego uznania – dokonanego przez stronę zastrzeżenia poufnego charakteru dostarczonych dokumentów i informacji, jako tajemnicy przedsiębiorstwa. W rezultacie druga strona postępowania może uzyskać dostęp do pełnego tekstu tych dokumentów, w tym informacji poufnych.

Prawo PUODO do uchylenia klauzuli poufności w odniesieniu do dokumentów lub ich części, które nie spełniają warunków tajemnicy przedsiębiorstwa jest nieprecyzyjne i w związku z tym odnośne decyzje PUODO mogą być traktowane jako uznaniowe. Biorąc pod uwagę nieodwracalną szkodę, jaka może

powstać w wyniku takiej decyzji, oraz brak możliwości odwołania się od decyzji, uprawnienie PUODO należy uznać za nieproporcjonalne i nieuzasadnione. Ponadto takie uprawnienie PUODO nie wprowadza odpowiedniej ochrony praw własności intelektualnej przysługujących stronie. Rekomendujemy usunięcie tego uprawnienia PUODO.

W przypadku, gdy usunięcie tego uprawnienia nie będzie możliwe konieczne jest wprowadzenie postanowienia, na mocy którego strona będzie mieć prawo do wystąpienia o rozstrzygnięcie sądowe. Projekt Ustawy nie przewiduje prawa strony do odwołania się do sądu administracyjnego od decyzji PUODO w sprawie zaklasyfikowania niektórych informacji jako nie będących tajemnicą przedsiębiorstwa. Takie prawo stanowiłoby skuteczną ochronę.

Zgodnie z art. 59 Projektu Ustawy (zob. uwagi w pkt 10 poniżej) każda decyzja PUODO wydana w toku postępowania podlega natychmiastowemu wykonaniu, z wyjątkiem administracyjnych kar pieniężnych. Należy to zmienić wprowadzając przepis stanowiący, że PUODO może wydać postanowienie, od którego strona może się odwołać do sądu administracyjnego.

*9. Postanowienia ograniczające zakres przetwarzania danych – art. 53 Projektu Ustawy*

**Rekomendacja: Wprowadzenie prawa do odwołania się w toku postępowania prowadzonego przez PUODO od postanowienia ograniczającego zakres przetwarzania danych osobowych.**

**Wyjaśnienie:**

Projekt Ustawy daje PUODO prawo do wydania postanowienia ograniczającego zakres przetwarzania danych osobowych przez podmiot kontrolowany. Postanowienie będzie obowiązywało nie dłużej niż do końca postępowania. Zgodnie z art. 60 Projektu Ustawy wszystkie postanowienia wydane w toku postępowania mogą być zaskarżone w drodze odwołania od decyzji.

W uzasadnieniu Projektu Ustawy stwierdza się, że celem tego postanowienia jest zapewnienie, aby wszystkie kwestie związane z poszczególnymi postępowaniami były rozpatrywane w ramach jednego postępowania sądownoadministracyjnego. Nie jest to wystarczające uzasadnienie dla tak restrykcyjnego przepisu, który może spowodować nieproporcjonalną szkodę lub koszty, których naprawienia przedsiębiorca nie będzie w stanie dochodzić w drodze postępowania cywilnego.

Analiza postępowań prowadzonych w 2015 roku wykazała, że przeciętne postępowanie w pierwszej instancji GIODO trwało 295 dni. Pomimo oczywistej intencji projektodawcy wydaje się, że terminy postępowań mogą jednak i w nowym porządku prawnym ulegać przedłużeniu – tym bardziej, że projektodawca nie przewidział żadnej sankcji dla PUODO za niezałatwienie sprawy w terminie. Ograniczenie zakresu przetwarzania danych osobowych przez tak długi czas może mieć nieodwracalne negatywne konsekwencje dla działalności administratora danych/podmiotu przetwarzającego dane.

Dlatego też w naszej ocenie należy zmienić Projekt Ustawy poprzez wprowadzenie prawa dla strony do odwołania się do sądu administracyjnego od postanowienia ograniczającego zakres przetwarzania danych osobowych w trakcie postępowania.

Ponadto nie jest jasne, dlaczego Projekt Ustawy wyłącza stosowanie art. 10 Kodeksu postępowania administracyjnego. Artykuł ten wyznacza podstawową zasadę postępowania administracyjnego, zgodnie z którą strony powinny zostać wysłuchane. Powód tego wyłączenia nie został wskazany w uzasadnieniu Projektu Ustawy.



10. Natychmiastowa wykonalność decyzji wydanych przez PUODO – art. 59

Projektu Ustawy

**Rekomendacja: Decyzjom PUODO nie powinien być nadawany rygor natychmiastowej wykonalności.**

**Wyjaśnienie:**

Nie ma wystarczającego uzasadnienia dla tego, aby wszystkie decyzje wydane przez PUODO podlegały natychmiastowej wykonalności. Projekt Ustawy wprowadza wyjątek od natychmiastowej wykonalności w odniesieniu do administracyjnych kar pieniężnych, ale wyjątek ten jest zbyt wąski.

W uzasadnieniu Projektu Ustawy stwierdzono, że wyjątek ten jest konieczny ze względu na wysokość administracyjnych kar pieniężnych. PUODO może jednak nakładać w swoich decyzjach inne obowiązki, które mogą być bardziej uciążliwe niż sama kara pieniężna.

Zgodnie z art. 55 ust. 1 Projektu Ustawy PUODO może w drodze decyzji wykorzystać uprawnienia naprawcze przyznane na mocy art. 58 ust. 2 pkt. b)-j) Rozporządzenia. Obejmują one uprawnienie np. do wprowadzenia czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania, nakazu zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej. W przypadku niewłaściwego zastosowania decyzje mogą mieć nieodwracalne i niekorzystne skutki dla ich adresatów. Natychmiastowo wykonalne decyzje tego rodzaju skierowane do przedsiębiorców, których kluczowe procesy biznesowe oparte są na przetwarzaniu danych osobowych mogą potencjalnie prowadzić do ogromnych strat.

Ponadto zgodnie z Rozporządzeniem osoby fizyczne i prawne mają *prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego dotyczącej tych osób* (art. 78 ust. 1 Rozporządzenia). Możliwość złożenia do sądu administracyjnego skargi na decyzję PUODO bez prawa żądania zawieszenia natychmiastowego wykonania decyzji nie może być traktowana jako *skuteczny środek ochrony prawnej*. Nakazy i obowiązki wynikające z decyzji będą miały wpływ na administratora danych/podmiot przetwarzającego dane od momentu jej wydania.

W związku z powyższym, Projekt Ustawy powinien zostać zmieniony w następujący sposób:

- Decyzje nie powinny posiadać rygoru natychmiastowej wykonalności. PUODO powinien mieć prawo (a nie obowiązek) do nadania swoim decyzjom rygoru natychmiastowej wykonalności.
- Należy opracować katalog okoliczności, w których PUODO może podjąć decyzje o nadaniu rygoru natychmiastowej wykonalności.
- Po wydaniu decyzji przez PUODO adresat decyzji powinien mieć prawo do zwrócenia się do sądu z wnioskiem o wstrzymanie natychmiastowego wykonania decyzji.

Uzasadnieniem tych zmian jest m. in. Kodeks postępowania administracyjnego, który stanowi podstawę prawną dla natychmiastowej wykonalności decyzji, np. ochrona życia i zdrowia, zabezpieczenie interesu narodowego lub innych interesów społecznych lub wyjątkowo ważnych interesów strony.

11. Brak ochrony przed nadmierną uciążliwością kontroli – art. 73 Projektu Ustawy

**Rekomendacja: Projekt Ustawy nie powinien wykluczać stosowania przepisów Ustawy o swobodzie działalności gospodarczej chroniącej przedsiębiorców przed nadmierną kontrolą.**

**Wyjaśnienie:**

Zgodnie z Projektem Ustawy, kontrola działalności gospodarczej przedsiębiorcy jest przeprowadzana zgodnie z Ustawą o swobodzie działalności gospodarczej. Projekt Ustawy wyklucza jednak stosowanie

przepisu mającego na celu ochronę przedsiębiorcy przed nadmierną kontrolą, tj. obowiązku powiadomienia przedsiębiorcy przez organ o zamiarze wszczęcia kontroli, zasady „jedna kontrola na raz”, maksymalnego czasu trwania wszystkich kontroli w ciągu jednego roku kalendarzowego.

W uzasadnieniu Projektu Ustawy wyjaśniono, że wyłączenie tych przepisów jest konieczne w celu zapewnienia wystarczającej ochrony danych osobowych oraz że stosowanie tych przepisów mogłoby wstrzymać rzetelne i terminowe prowadzenie postępowania. Autorzy Projektu Ustawy stwierdzają, że nie powinna mieć miejsca sytuacja, w której kontrola prowadzona przez inny organ mogłaby uniemożliwić PUODO przeprowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych. W tej sytuacji ochrona prawa podstawowego jakim jest prawo do ochrony danych osobowych, mogłaby stać się iluzoryczna.

Prawo do ochrony danych osobowych jest bez wątpienia prawem podstawowym, ale nie powinno być traktowane jako prawo bezwarunkowe.

Przepisy Ustawy o swobodzie działalności gospodarczej zostały stworzone w celu ochrony konstytucyjnego prawa do prowadzenia działalności gospodarczej. Ponadto przepisy te mają na celu zapewnienie, aby kontrole były przeprowadzane w możliwie najbardziej efektywny sposób zarówno dla organów, jak i przedsiębiorców. Dwie lub więcej równoczesnych kontroli mogą być nadmiernym obciążeniem dla przedsiębiorcy, a nawet osiągnąć skutek przeciwny do zamierzonego.

Projekt Ustawy zapewnia ochronę zarówno osobom, których dane dotyczą, jak i administratorom danych. Jednakże wyłączenie przepisów chroniących przed nadmierną liczbą kontroli jest sprzeczne z dążeniem PUODO do przeprowadzenia przezeń skutecznych kontroli, które umożliwią przedsiębiorcom dostarczanie organowi wszelkich niezbędnych dokumentów i informacji.

Projekt Ustawy nadaje PUODO nadmierne uprawnienia kontrolne. Zgodnie z proponowaną zmianą możliwe będzie przesłuchanie pracownika podmiotu kontrolowanego w charakterze świadka pod rygorem odpowiedzialności karnej za zeznanie nieprawdy lub zatajenie prawdy. Uprawnienie to jest będzie stanowiło nieproporcjonalną i nadmierną uciążliwość dla pracowników.

Ponadto, Projekt Ustawy daje PUODO prawo do ustalenia terminu na dostarczenie dowodu będącego w posiadaniu strony. Termin na przedstawienie takiego dowodu nie może być krótszy niż 7 dni. Uzyskanie dowodu w tak krótkim terminie, może być dla międzynarodowych przedsiębiorstw niezwykle trudne.

*12. Niższe administracyjne kary pieniężne dla podmiotów publicznych – art. 83  
Projektu Ustawy*

**Rekomendacja: Nie powinno być tak istotnego rozróżnienia między podmiotami publicznymi a prywatnymi w odniesieniu do administracyjnych kar pieniężnych.**

**Wyjaśnienie:**

W Projekcie Ustawy maksymalna administracyjna kara pieniężna dla podmiotów publicznych wynosi 100 tys. zł. Nie ma wystarczającego uzasadnienia dla ograniczenia odpowiedzialności finansowej organów publicznych za naruszenie przepisów o ochronie danych osobowych.

Rozporządzenie daje państwom członkowskim uprawnienie do ustanawiania zasad określających, czy i w jakim zakresie można nakładać administracyjne kary pieniężne na organy publiczne. Nie ma jednak żadnego uzasadnienia dla tak idącego zróżnicowania pomiędzy podmiotami publicznymi i prywatnymi.

W uzasadnieniu Projektu Ustawy stwierdza się, że podmioty publiczne są finansowane z budżetu państwa, a administracyjne kary pieniężne stanowią dochody budżetu państwa. Administracyjna kara

pieniężna nałożona na organ publiczny stanowi zatem przeniesienie środków w ramach administracji publicznej. Nie zgadzamy się z takim podejściem.

Maksymalna administracyjna kara pieniężna jest tak niska, że może skłonić decydentów w organach publicznych do wyciągnięcia wniosku, że bardziej korzystne będzie zapłacenie kary pieniężnej (nawet w maksymalnej wysokości) niż inwestowanie w środki techniczne i organizacyjne chroniące dane osobowe obywateli. Proponowane rozwiązanie drastycznie obniża poziom ochrony danych osobowych w organach publicznych, co jest sprzeczne z całą koncepcją Rozporządzenia i podejmowaną reformą ochrony danych osobowych. Organy publiczne przetwarzają nierzadko ogromne zbiory danych, w tym wrażliwych danych osobowych obywateli. Ponieważ dotychczas obowiązujące przepisy karne dotyczące ochrony danych i ochrony przed bezprawnym wykorzystaniem zostaną usunięte (bez wprowadzania nowych przestępstw), sektor publiczny nie będzie miał żadnej motywacji do priorytetowego traktowania kwestii ochrony danych.

Projekt Ustawy powinien zostać zmieniony w celu usunięcia (tak istotnego) zróżnicowania maksymalnych administracyjnych kar pieniężnych.

### **Projekt ustawy – przepisy wprowadzające ustawę o ochronie danych osobowych z dnia 12 września 2017 roku**

#### **Projekt zmian w Kodeksie Pracy**

##### *13. Gromadzenie biometrycznych danych osobowych w miejscu pracy – art. 22<sup>2</sup> § 2 Kodeksu Pracy*

**Rekomendacja: Przepisy regulujące przetwarzanie danych biometrycznych powinny być bardziej precyzyjne.**

##### **Wyjaśnienie:**

Projekt zmian w Kodeksie Pracy stanowi, że przetwarzanie danych biometrycznych jest dozwolone tylko wtedy, gdy dane dotyczą stosunku pracy i gdy pracownik wyraził zgodę na takie przetwarzanie.

Użycie terminu *dotyczące stosunku pracy* nie zapewnia pracodawcom wystarczającej jasności co do sposobu odróżnienia takich danych od innych podobnych danych.

Zalecamy usunięcie tego terminu, ponieważ może powodować on rozbieżne interpretacje.

##### *14. Korzystanie z monitoringu wizyjnego (CCTV) w miejscu pracy – art. 22<sup>4</sup> Kodeksu Pracy*

**Rekomendacja: Przepisy regulujące korzystanie z systemów monitoringu wizyjnego powinny być bardziej precyzyjne.**

##### **Wyjaśnienie:**

Zgodnie z proponowanymi zmianami, stosowanie monitoringu wizyjnego będzie dozwolone tylko wtedy, gdy jest ono konieczne dla zapewnienia bezpieczeństwa pracowników, ochrony mienia lub zachowania w tajemnicy informacji. Brak jest innych powodów, uzasadniających korzystanie z systemu monitoringu wizyjnego. Ograniczenie to nie powinno zostać utrzymane. Istnieje wiele możliwych powodów, dla których warto korzystać z systemu monitoringu wizyjnego, które nie zostały uwzględnione w tym katalogu. Dlatego też należy zmienić ten przepis poprzez dodanie klauzuli „w szczególności”.



Nowelizacja stanowi, że systemy monitoringu wizyjnego nie mogą być wykorzystywane jako środek kontroli wykonywania pracy przez pracowników. Zakres tego pojęcia jest zbyt szeroki i niejasny. Wiele działań pracodawcy w stosunku do pracowników opierają się na konieczności nadzoru nad wykonywaną przez nich pracą. W praktyce PUODO może interpretować ten termin zbyt szeroko, ograniczając tym samym możliwość korzystania przez pracodawców z systemów monitoringu wizyjnego w rozsądnych celach biznesowych. Proponujemy wprowadzenie innego sformułowania, skoncentrowanego na zrównoważeniu uzasadnionych praw zarówno pracodawców, jak i pracowników, którzy nie powinni być poddawani *inwazyjnym* lub *nadmiernym* kontrolom w rozumieniu ich poszanowania prawa do prywatności w miejscu pracy.

Po drugie, proponowany projekt nie mówi nic o monitorowaniu komunikacji elektronicznej pracowników, co w praktyce jest bardziej powszechnym zjawiskiem niż systemy monitoringu wizyjnego. Dlatego też nie jest zrozumiałym, dlaczego projektodawca zdecydował się uregulować sferę CCTV, pozostawiając monitoring komunikacji elektronicznej bez żadnej regulacji. Proponujemy dodanie przepisu umożliwiającego pracodawcom monitorowanie komunikacji elektronicznej w zakresie wymaganym do ochrony informacji poufnych lub bezpieczeństwa danych. Brzmienie tekstu powinno być zgodne z zasadami określonymi w Opinii 2/2017 Grupy Roboczej Artykułu 29 ds. Ochrony Danych w sprawie przetwarzania danych w miejscu pracy.

Ponadto proponowane zmiany stanowią, że system monitoringu wizyjnego nie powinien obejmować pomieszczeń nieprzeznaczonych do pracy, w szczególności pomieszczeń sanitarnych, szatni, stołówek i palarni. Zastosowanie systemów monitoringu wizyjnego w stołówce można jednak uzasadnić względami bezpieczeństwa, np. szybszym reagowaniem na wypadki. Obecnie często zdarza się, że pomieszczenia przeznaczone do spożywania posiłków są dzielone z innymi (otwartymi) pomieszczeniami biurowymi, które wymagają monitorowania (np. drzwi wejściowe do biura).

W związku z tym przepisy dotyczące systemów monitoringu wizyjnego powinny być przeanalizowane pod kątem potrzeby zapewnienia ochrony zarówno pracownikom jak i pracodawcom.