



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Jan Nowak

Do druku nr 970

Warszawa, 11 marca 2021 r.

DOL.401.81.2021.WL.MP

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu
Kancelaria Sejmu RP
ul. Wiejska 4/6/7
00-902 Warszawa
ESP: /KSRP/SKRYTKAES

Szanowny Panie Ministrze,

w nawiązaniu do pisma z 23 lutego 2021 r. (sygn. SPS-WP.020.51.4.2021) uprzejmie dziękuję za przedstawienie rządowego projektu ustawy o zmianie ustawy o Karcie Dużej Rodziny, ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz ustawy o opiece nad dziećmi w wieku do lat 3 do zaopiniowania przez organ właściwy w sprawie ochrony danych osobowych oraz uprzejmie informuję, że – z punktu widzenia przepisów 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 z 04.05.2016, str. 1, z późn. zm.¹) – do niniejszego projektu, zwanego dalej projektem ustawy, zgłaszam następujące uwagi.

1. **Uwaga do art. 1 pkt 1 projektu ustawy formułującego nowe brzmienie art. 2 pkt 2 ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (Dz. U. z 2020 r. poz. 1348, z późn. zm.), zwanej dalej ustawą o KDR, poprzez jego podział na lit. a) i b).**

Projektodawca proponuje aby przepis art. 2 pkt 2 lit. a) ustawy o KDR brzmiał następująco: „*Karta jest środkiem identyfikującym członka rodziny wielodzietnej, poświadczającym*

¹ Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35.

prawo członka rodziny wielodzietnej do uprawnień ustalonych w trybie określonym w niniejszej ustawie lub przyznanych na podstawie przepisów odrębnych realizowanym przy użyciu oprogramowania dedykowanego dla urządzeń mobilnych, zawierającego usługi ułatwiające korzystanie z przyznanych uprawnień, udostępnionego przez ministra właściwego do spraw rodziny, lub wskazanego w informacji zamieszczonej na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw rodziny.”.

Kwestia oprogramowania dedykowanego dla urządzeń mobilnych, zawierającego usługi ułatwiające korzystanie z przyznanych uprawnień, udostępnionego przez ministra właściwego do spraw rodziny została uregulowana ustawą z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. z 2018 r. poz.1544, z późn. zm.). Obecnie tym oprogramowaniem dedykowanym dla urządzeń mobilnych jest Aplikacja mKDR, która wskazywana jest w informacji zamieszczonej na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw rodziny.

Niemniej jednak, z obecnych przepisów ustawy o KDR, jak i z zaproponowanych przez Projektodawcę zmian nie wynika wprost kto jest administratorem przetwarzanych w aplikacji danych, jakie dane przetwarzane są w tej aplikacji i w jakim celu, przez jaki okres czasu, jakie są procesy przetwarzania danych osobowych, w tym skąd są one pozyskiwane i jakim podmiotom udostępniane. Warto również zauważyć, że odpowiedzi na powyższe kwestie częściowo można znaleźć jedynie w klauzuli informacyjnej zamieszczonej w Biuletynie Informacji Publicznej Ministerstwa Rodziny i Polityki Społecznej, gdyż w zakładce strony internetowej Ministerstwa Rodziny i Polityki Społecznej dedykowanej dla tej aplikacji nie można odnaleźć regulaminu określającego jej działanie. Nie jest jasne również jaki system teleinformatyczny umożliwia obsługę funkcjonalności związanych z kartami elektronicznymi, które pozwalają na potwierdzenie uprawnień członków rodzin wielodzietnych oraz zapewniają usługi ułatwiające korzystanie z uprawnień przyznanych na podstawie Karty Dużej Rodziny. Dla porównania warto zwrócić uwagę jak szczegółowo – w stosunku do Aplikacji mKDR – uregulowane zostało działanie publicznej aplikacji mobilnej (mObywatel) w art. 19e i następnych ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, z późn. zm.), która również będzie pozwalać na obsługę elektronicznych Kart Dużej Rodziny.

Ustawa o KDR wymaga zatem zapewnienia w treści jej przepisów kompleksowej regulacji doprecyzowującej kwestię przetwarzania danych w Aplikacji mKDR pod kątem zasad dotyczących przetwarzania danych osobowych zawartych w art. 5², w tym zasady zgodności z prawem,

²Art. 5 ust. 1. Dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”); b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”); d) prawidłowe i w razie potrzeby uaktualniane („prawidłowość”); e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w

rzetelności i przejrzystości oraz przesłanek przetwarzania danych przez organy publiczne wskazanych w art. 6 ust. 1 lit. c)³ i e)⁴ ogólnego rozporządzenia o ochronie danych. Przejrzyste i wyczerpujące określanie praw i obowiązków wiążących organy i podmioty z sektora administracji sprzyja stosowaniu ww. zasady legalizmu (niedomniemywaniu kompetencji), co w konsekwencji eliminuje wątpliwości związane z praktycznym stosowaniem przepisów prawa.

2. Uwaga do art. 1 pkt c projektu ustawy dodającego ust. 19a do art. 10 ustawy o KDR w związku z art. 6 projektu ustawy.

Projektodawca proponuje aby przepis **art. 10 ust. 19a ustawy o KDR** brzmiał następująco:
„Minister właściwy do spraw informatyzacji po otrzymaniu od ministra właściwego do spraw rodziny informacji dotyczących osób, którym przyznano Kartę, niezwłocznie przekazuje mu posiadane dane z rejestru PESEL w zakresie daty zgonu albo daty znalezienia zwłok członka rodziny wielodzietnej, w celu umożliwienia wójtowi weryfikacji prawa do Karty.”. Natomiast zgodnie z art. 6 ust. 1 przepisy **art. 10 ust. 19a ustawy** zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą mają zastosowanie po raz pierwszy po wdrożeniu rozwiązań technicznych umożliwiających uzyskanie przez ministra właściwego do spraw rodziny od ministra właściwego do spraw informatyzacji informacji, o której mowa w art. 10 ust. 19a ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, oraz przekazanie jej wójtom, burmistrzom i prezydentom miast.

Dla realizacji celów przekazywania danych osobowych pomiędzy określonymi podmiotami będącymi organami publicznymi istotne jest określenie w przepisach prawa sposobu ich przekazywania co ma bezpośredni wpływ na bezpieczeństwo ich przetwarzania i realizację zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych) oraz zasady integralności i poufności (art. 5 ust. 1 lit. f ogólnego rozporządzenia o ochronie danych).

Zasada integralności i poufności stanowi, że *przetwarzane danych powinno odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed*

których dane te są przetwarzane („ograniczenie przechowywania”); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

Ust. 2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

³Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

⁴Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi

niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Projektodawca powinien wyczerpująco dookreślić w projektowanych przepisach cele przetwarzania danych osobowych, odpowiadające tym celom role organów / podmiotów uczestniczących w procesach przetwarzania danych osobowych (administrowanie – art. 4 pkt7⁵/ współadministrowanie – art. 26⁶ ogólnego rozporządzenia o ochronie danych) oraz zasady i sposoby przetwarzania danych osobowych na potrzeby wypełnienia celów regulacji ustawy o KDR, w tym jak będzie wyglądał przepływ danych pomiędzy ministrem właściwym do spraw informatyzacji, ministrem właściwym do spraw rodziny oraz wójtami w celu weryfikacji prawa do Karty Dużej Rodziny, czy zastosowanie będzie miał system teleinformatyczny już wykorzystywany przez ministra właściwego do spraw informatyzacji, czy będzie to nowy system teleinformatyczny, jak będzie odbywało się wnioskowanie o dane do ministra właściwego do spraw informatyzacji i przekazywanie już przetworzonych danych do ministra właściwego do spraw rodziny i dalej do wójtów, burmistrzów i prezydentów miast.

Organ nadzorczy przypomina także o wymogu przeprowadzenia oceny skutków dla ochrony danych⁷ w odniesieniu do planowanego przetwarzania danych osobowych z użyciem nowoczesnych technologii, tj. za pośrednictwem publicznej aplikacji mobilnej (mObywatel) oraz w odniesieniu do już przeprowadzanego procesu przetwarzania danych, które odbywa się za pośrednictwem Aplikacji mKDR. Uzasadnienie do projektu ustawy takiej oceny skutków dla ochrony danych nie zawiera, a zatem brak jest informacji o przeprowadzaniu takiej oceny, oraz analizy ryzyk i wpływu ich wyników na przyjmowane rozwiązania dotyczące przetwarzania danych osobowych, w tym ich szczególnych kategorii (art. 9 ogólnego rozporządzenia o ochronie danych) z użyciem

⁵„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.

⁶Art. 26 ust. 1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą

⁷Art. 35 ust. 1 w związku z ust. 10 ogólnego rozporządzenia o ochronie danych reguluje obowiązek dokonania – przed rozpoczęciem przetwarzania – oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Ocena skutków dla ochrony danych nie jest wymagana jeżeli operacja przetwarzania, zgodnie z art. 6 ust. 1 lit. c) lub e) ogólnego rozporządzenia o ochronie danych, ma podstawę prawną w prawie UE lub w prawie państwa członkowskiego, które reguluje daną operację przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej. Zgodnie z art. 35 ust. 7 ogólnego rozporządzenia o ochronie danych, ocena skutków zawiera co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania; ocenę, czy operacje są niezbędne oraz proporcjonalne w stosunku do celów; ocenę ryzyka naruszenia praw lub wolności podmiotów danych; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych i wykazać przestrzeganie ogólnego rozporządzenia o ochronie danych.

nowoczesnych technologii. Taka ocena skutków powinna być przeprowadzona, a wypływające z niej wnioski powinny mieć wpływ na przyjmowane przez projektodawcę rozwiązania z zakresu przetwarzania danych osobowych. Ocena powinna obejmować planowane operacje przetwarzania i cele przetwarzania; ocenę, czy operacje są niezbędne oraz proporcjonalne w stosunku do celów regulacji wynikających z ustawy o KDR; ocenę ryzyka naruszenia praw lub wolności podmiotów danych – beneficjentów ustawy o KDR; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych i wykazać przestrzeganie ogólnego rozporządzenia o ochronie danych przez administratora (-ów) (współadministratorów), tj. organy/podioty będące wykonawcami norm ustawy o KDR. Jej przeprowadzenie wykazałoby potrzebę przetwarzania konkretnych danych albo jej brak jak również opisywałaby w pełni proces ich przetwarzania co pozwala na wykazanie przez administratora (współadministratora) przestrzegania zasad przetwarzania danych zgodnie z ww. zasadą rozliczalności sformułowaną w art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych. Dodatkowo warto zauważyć, że sporządzenie takiej oceny również dla planowanego przetwarzania danych na podstawie projektowanego art. 10 ust. 19a dodawanego do ustawy o KDR pomogłoby w sporządzeniu schematu przepływu i sposobu przetwarzania danych, co pozwoliłoby na sformułowanie odpowiednich przepisów określających ten proces.

Z wyrazami szacunku,

Prezes Urzędu
Ochrony Danych Osobowych
Jan Nowak

/-dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym- /