|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tabela uwag**  **zgłoszonych do projektu rozporządzenia Ministra Cyfryzacji w sprawie prowadzenia Rejestru Dowodów Osobistych**  **w ramach opiniowania** | | | | |
| lp. | **Podmiot wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Zgłoszone uwagi** | **Stanowisko** |
|  | **PKN** | §4 ust**.** 3 | W § 4 ust. 3 projektu rozporządzenia została powołana norma PN-EN 419211-2:2013. Należy pamiętać, że zgodnie z art. 5 ust. 3 ustawy o normalizacji z dnia 12 września 2002 r. stosowanie Polskich Norm jest dobrowolne. Nakładanie obowiązku stosowania Polskich Norm w drodze rozporządzenia jest niezgodne z ustawą o normalizacji jak i rozporządzeniem o normalizacji europejskiej1 oraz z regułami legislacyjnymi. Odniesienie się do normy w akcie prawnym niższego rzędu niż ustawa nie jest wystarczającą przesłanką do stwierdzenia obowiązku jej stosowania.  Jednocześnie informuję, że prawidłowy nr referencyjny powołanej w par. 4. ust. 3 normy to PN-EN 419211-2:2013-11. | **Uwaga wyjaśniona**  W przepisach rozporządzenia, które dotyczą kwestii związanych z szyfrowaniem danych biometrycznych w zakresie odcisków palców przywołane zostały normy ETSI, których stosowanie ma wprawdzie charakter dobrowolny, jednakże ich przywołanie w niniejszym projekcie wynikało z wymagań artykułu 11 ust.1 rozporządzenia PE i Rady (UE) 2019/1157 „Bez uszczerbku dla rozporządzenia (UE) 2016/679 państwa członkowskie zapewniają bezpieczeństwo, integralność, autentyczność i poufność danych gromadzonych i przechowywanych na użytek niniejszego rozporządzenia”. Zgodnie z rozporządzeniem wprowadzono mechanizmy ochrony danych nie tylko w samym nośniku (warstwie elektronicznej) dowodu osobistego, ale również w systemach, w których są one przetwarzane.  Norma EN 419211-2: 2013 – Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu – Część 2: Urządzenie z generowaniem kluczy, jest technicznym opisem profilu wymagań dla urządzenia, które powinno być zastosowane w celu zagwarantowania właściwego poziomu ochrony i poufności przetwarzanych danych w systemie. Poziom bezpieczeństwa wynikający z zapisów normatywnych jest przywołany np. w decyzji wykonawczej Komisji (UE) 2016/650 do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014.  Norma ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates, reguluje zasady wydawania certyfikatów, które są elementem mechanizmów bezpieczeństwa (potwierdzenia pochodzenia i przynależności kluczy), bez których utrzymanie oczekiwanego poziomu poufności danych nie byłoby możliwe. |
|  | **PKN** | **§4 ust. 4** | Powołana w par. 4. ust. 4 norma ETSI EN 319 411 to w rzeczywistości seria norm:  ETSI EN 319 411-1 V1.2.2:2018  ETSI EN 319 411-2 V2.2.2:2018  ETSI EN 319 411-3 V1.1.1:2013  Proponowany zapis: „Potwierdzenie wiarygodności kluczy jest realizowane z wykorzystaniem certyfikatu klucza publicznego wydanego w ramach polityki certyfikacji spełniającej wymagania określone w normach wprowadzających serię norm ETSI EN 319 411.” | **Uwaga uwzględniona**  § 4 ust. 4 nadano brzmienie proponowane przez Polski Komitet Normalizacyjny |
|  | **UODO** | **§ 4 ust. 5** | dane biometryczne w zakresie odcisków palców mogą być przetwarzane w postaci niezaszyfrowanej w trakcie procesu ich pobierania oraz personalizacji dowodu osobistego nie określa mechanizmów ochrony procesów przetwarzania danych biometrycznych w takiej formie. Projektodawca powinien przewidzieć, choćby kierunkowo, jakie mechanizmy zostaną zastosowane w celu zapewnienia skutecznej ochrony przed nieuprawnionym dostępem do niezaszyfrowanych danych. Zgodnie z opinią Grupy Roboczej Art. 29 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych „Administratorzy danych muszą wprowadzić odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania”. Brak uregulowania powyższych kwestii budzi obawy związane z ryzykiem nienależytego zabezpieczeniem przetwarzanych danych osobowych biometrycznych. | **Uwaga wyjaśniona**  Z uwagi na fakt, że nie ma możliwości zapisania odcisków palców na żadnym znanym w chwili obecnej nośniku informatycznym, celem przeniesienia ich w sposób bezpieczny i integralny przez organ do RDO, przepis został wykreślony. Powyższe jest również konsekwencją zastosowanych przy pobieraniu odcisków palców mechanizmów, o czym mowa w wyjaśnieniu do §4 ust. 6. |
|  | **UODO** | **§ 4 ust. 6** | Minister właściwy do spraw informatyzacji zapewnia stosowanie mechanizmów, które zapewniają ochronę przed nieuprawnionym dostępem do tych danych, w tym w szczególności ich kopiowanie, oraz zapewniają rejestrowanie wszelkich działań dokonywanych na tych danych” wymaga dookreślenia poprzez wskazanie zamkniętego katalogu mechanizmów zapewniających danym osobowym należyte zabezpieczenie. | **Uwaga wyjaśniona**  Na wstępie wskazać należy, ze przepis został zmodyfikowany z uwagi na fakt, że za przetwarzanie danych biometrycznych w procesie wydawania dowodów osobistych, na różnych etapach tego procesu (pobieranie odcisków palców oraz personalizacja dokumentów) odpowiedzialność ponosi dwóch ministrów: minister właściwy do spraw informatyzacji oraz minister właściwy do spraw wewnętrznych. Zaproponowano zatem następujące brzmienie przepisu: „*W przypadku, o którym mowa w ust. 5, minister właściwy do spraw informatyzacji oraz minister właściwy do spraw wewnętrznych, każdy w zakresie swojej właściwości, zapewniają* ***stosowanie mechanizmów****, które gwarantują ochronę przed nieuprawnionym dostępem do tych danych, w tym w szczególności ich kopiowanie, oraz zapewniają rejestrowanie wszelkich działań dokonywanych na tych danych*.”.  Odnosząc się już bezpośrednio do uwagi UODO wskazać należy, że owe **mechanizmy** dotycząkwestii technicznych jak i organizacyjnych leżących po stronie podmiotów które biorą czynny udział w procesie wydawania dowodów osobistych. Kwestie techniczne to zakup przez Ministra Cyfryzacji skanera linii papilarnych, który umożliwia bezpieczne pobranie odcisków palców, natomiast kwestie organizacyjne to chociażby zapewnienie takiej lokalizacji stanowiskobsługującychsprawy dowodowe aby uniemożliwić dostęp osób nieuprawnionych. Wydaje się niecelowym tworzenie w przepisach rangi rozporządzenia zamkniętego katalogu takich mechanizmów, chociażby z uwagi na fakt, że zmiana poszczególnych elementów zastosowanych mechanizmów powodowałaby konieczność zmiany aktu prawnego. Ponadto należy wskazać, ze w obecnie funkcjonujących przepisach prawa mamy do czynienia właśnie w zakresie grupy przepisów dot. przetwarzania danych osobowych podobnie sformułowane przepisy w zakresie wymagań, które musza spełnić podmioty aby otrzymać dostęp do danych w trybie teletransmisji. Przepis mówi o konieczności spełnienia przez nie warunków technicznych i organizacyjnych, bez wskazani na konkretny katalog tych warunków. |
|  | **Wielkopolski Urząd Wojewódzki** | **§ 5 pkt 2** | Wyjaśnienia wymaga:   1. Tryb/sposób przekazywania danych (w szczególności odcisków palców) do ministra właściwego do spraw wewnętrznych na bezpiecznym nośniku informatycznym;   Czy brak dostępu do RDO nie będzie uniemożliwiać przyjmowania wniosków o dowód osobisty i wydawania dokumentów? | **Uwaga uwzględniona**  Wskazane przepisy zostały zmienione |
|  | **Wojewoda Warmińsko - Mazurski** | **§ 5 pkt 2** | Należałoby rozważyć zmianę użytych w projekcie sformułowań: zawieszenie/cofnięcie zawieszenia dowodu osobistego, bowiem ustawa z dnia z 6 sierpnia 2010 r. o dowodach osobistych, stanowiąca podstawę do wydania projektowanego rozporządzenie Ministra Cyfryzacji nie posługuje się takimi pojęciami. W ustawie o dowodach osobistych użyto określenia „zawieszanie/cofanie zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego”. Powyższe oznacza, że zawieszeniu podlegają nie dowody osobiste, a certyfikaty zamieszczone w warstwie elektronicznej dowodu osobistego | **Uwaga uwzględniona**  Wskazane przepisy zostały zmienione |