

Warszawa, 20-01-2021



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Jan Nowak

DOL.401.12.2021.WL.PM

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU

L.dz. *SPS-WP.020.4.16.2021*.....

Data wpływu *21.01.21*.....

Pan

Dariusz Salomończyk

Zastępca Szefa Kancelarii Sejmu

ul. Wiejska 4/6/8

00-902 Warszawa

elektroniczna skrzynka podawcza ePUAP

/KSRP/SkrytkaESP

Szanowny Panie Ministrze,

w związku z korespondencją z dnia 12 stycznia 2021 r. (znak: SPS-WP.020.4.5-2021) przekazującą do zaopiniowania poselski projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (druk sejmowy nr 867), Prezes Urzędu Ochrony Danych Osobowych, z punktu widzenia przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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⁾), dalej: rozporządzenie 2016/679, zgłasza następujące uwagi.

1. **Art. 1 pkt 1 projektowanej ustawy nadaje nowe brzmienie art. 255a § 2 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2020 r. poz. 1444 i 1517), dalej KK.** Zgodnie z nowoprojektowanym art. 255a § 2 KK *Tej samej karze podlega, kto w celu popełnienia przestępstwa o charakterze terrorystycznym uczestniczy w szkoleniu mogącym umożliwić popełnienie takiego przestępstwa lub samodzielnie zapoznaje się z treściami, o których mowa w § 1.* Art. 255a § 1 KK stanowi natomiast: *Kto rozpowszechnia lub publicznie prezentuje treści mogące ułatwić popełnienie przestępstwa o charakterze terrorystycznym w zamiarze, aby przestępstwo takie zostało popełnione, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

¹⁾ Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

Charakter nowoprojektowanego art. 255a § 2 KK może prowadzić do sytuacji kiedy to organy ścigania – w wyniku wykrycia czynu z 255a § 1 KK, tj np. rozpowszechniania danego materiału poprzez sieć Internet – będą podejmować działania operacyjne wobec osób, które nawet w sposób przypadkowy i niezamierzony zapoznały się z tymi treściami. Dlatego też, art. 255a § 2 KK powinien dookreślać, że penalizowaniu podlega zapoznawanie się z treściami, o których mowa w art. 255a § 1 KK, jeśli osobie, która z nimi się zapoznaje towarzyszy zamiar popełnienia przestępstwa o charakterze terrorystycznym.

Taka konstrukcja art. 255a § 2 KK przyczyni się do stworzenia pełniejszej gwarancji ochrony prywatności osób korzystających z sieci Internet, penalizując wyłącznie osoby, które zapoznają się z danymi treściami znając w pełni ich kontekst. Przyjęcie takiego rozwiązania przyczyni się do stosowania art. 10 rozporządzenia 2016/679² oraz zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679³).

2. Zgodnie z art. 2 pkt 2 lit. a projektowanej ustawy nadającym nowe brzmienie art. 218 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2020 r. poz. 30, 413, 568, 1086 i 1458) *Urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną lub świadczące usługi drogą elektroniczną oraz dostawcy usług cyfrowych obowiązani są niezwłocznie zabezpieczyć, na żądanie sądu lub prokuratora zawarte w postanowieniu, na czas określony, nieprzekraczający jednak 90 dni, dane informatyczne przechowywane w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym. W sprawach o przestępstwa określone w art. 200b, art. 202 § 3, 4, 4a, 4b lub art. 255a Kodeksu karnego oraz w rozdziale 7 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz. U. z 2020 r. poz. 2050) zabezpieczenie może być połączone z obowiązkiem uniemożliwienia dostępu do tych danych. Przepis art. 218 § 2 zdanie drugie stosuje się odpowiednio.*

Konstrukcja projektowanego przepisu nie wskazuje w jaki sposób będzie realizowany obowiązek „uniemożliwienia dostępu do tych danych”. Nie wiadomo czy dotyczyć on będzie wyłącznie nośnika na jakim zostały zabezpieczone te dane, uniemożliwienia

² 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.

³ Zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

dostępu do nich danej osobie, której dotyczy żądanie sądu lub prokuratora czy też wszystkich osób, którym przedsiębiorca świadczy usługi.

Rozwiązania w tym zakresie są konieczne dla właściwego stosowania art. 10 rozporządzenia 2016/679 oraz zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679).

3. Zgodnie z art. 2 pkt 8 projektowanej ustawy dodającym nowy § 2a w art. 334 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego: *Odpisy aktu oskarżenia, o których mowa w § 2 pkt 2, mogą być przesłane sądowi w postaci elektronicznej, z wyłączeniem odpisów przeznaczonych dla adresatów, którzy w dniu przesłania sądowi aktu oskarżenia są pozbawieni wolności lub których adresu poczty elektronicznej nie ustalono.* Z projektowanego przepisu wynika, że odpis aktu oskarżenia będzie mógł być przesyłany adresatowi za pośrednictwem poczty elektronicznej. Proponowane brzmienie przepisów wywołuje wątpliwości. Po pierwsze, w jaki sposób ten adres będzie od oskarżonego pozyskiwany oraz czy będzie on przekazywany przez niego dobrowolnie czy też ustalany w ramach działań operacyjno-rozpoznawczych. Po drugie, istotnym jest czy Projektodawca przeanalizował wszystkie zagrożenia dla bezpieczeństwa danych osobowych, w szczególności poufności komunikacji, za pośrednictwem poczty elektronicznej, zgodnie z zasadą integralności i poufności (art. 5 ust. 1 lit. f RODO⁴), a w konsekwencji czy dokonana w tym zakresie analiza pozwala na przyjęcie, że proponowane przepisy w ocenie Projektodawcy dają wystarczające gwarancje wykonywania proponowanych norm w sposób zapewniający stosowanie rozporządzenia 2016/679.
4. Zgodnie z art. 2 pkt 11 projektowanej ustawy dodającym nowy art. 310a w ustawie z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego *Minister Sprawiedliwości może zawrzeć z odpowiednim organem państwa obcego porozumienie przewidujące podział kwot lub przedmiotów uzyskanych z wykonania orzeczenia skazującego na grzywnę lub z orzeczenia przepadku, o których mowa w art. 609 § 4 oraz art. 610 § 4 i 5.* O ile w ramach ww. porozumienia będzie dochodziło do przekazywania danych osobowych to uzasadnionym jest rozważanie przez Projektodawcę wskazania minimalnych gwarancji w przepisach powszechnie obowiązujących co do wymaganych elementów porozumienia w zakresie stosowania przepisów rozporządzenia 2016/679. Nieprzyjęcie takiego

⁴ Zgodnie z zasadą integralności i poufności dane osobowe muszą być 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.

rozwiązania oznaczać będzie obarczenie Ministra Sprawiedliwości odpowiedzialnością za przyjmowanie w każdym porozumieniu rozwiązań/postanowień zapewniających stosowanie przepisów rozporządzenia 2016/679, z rozróżnieniem sytuacji kiedy porozumienie zawierane będzie z organami państwa związanego przepisami ogólnego rozporządzenia o ochronie danych oraz sytuacji zawierania porozumienia z organem funkcjonującym w porządku prawnym państwa trzeciego, co ma szczególne znaczenia dla transferów danych osobowych, do których zastosowanie będzie miał Rozdział V RODO *Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych.*

Z wyrazami szacunku,

Prezes Urzędu Ochrony Danych Osobowych
Jan Nowak
/ - podpisano elektronicznie/