https://doi.org/10.31268/ZPBAS.2018.67 nr 4(60) 2018 ▪ s. 108–117 ZESZYTY PRAWNICZE BAS Biura Analiz Sejmowych Kancelarii Sejmu

Martyna Kusak

Ocena rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy nr 2989) pod kątem bezpieczeństwa gromadzenia, przechowywania, przesyłania i dostępu do danych osobowych[1]

Assessment of governmental Bill on the Protection of Personal Data Processed in Relation to the Prevention of and Fighting Crime (Sejm's Paper no. 2989) in terms of security of collection, storage, transmission and access to personal data: Most of the legal solutions proposed in the bill are in line with the standards of Directive 2016/680 in the context of the security of collection, storage, transmission and access to personal data, and guarantees data security. However, in a number of places, the reviewed bill includes solutions that do not guarantee the security of personal data. These are, among others, Article 19 of the bill, which has not been used to increasing the data security, or Article 17 of the bill, which does not protect against reverse pseudonymisation. Gaps regarding data protection lacunas also appear in the bill, inter alia, in its Article 41, which is too narrow in terms of the scope of data processing and authorization to processing.

Keywords: personal data protection, bill, crime, European Union

Słowa kluczowe: ochrona danych osobowych, projekt ustawy, przestępczość, Unia Europejska

Doktor nauk prawnych, Wydział Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu ▪ m.kusak@amu.edu.pl ▪ https://orcid.org/0000-0002-7596-9022

[1] *Opinia prawna w przedmiocie rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk nr 2989) pod kątem bezpieczeństwa gromadzenia, przechowywania, przesyłania i dostępu do danych osobowych* sporządzona 29 listopada 2018 r. na zlecenie Biura Analiz Sejmowych; BAS 2768/18.

Przedmiot opinii

Rządowy projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[2] (dalej: projekt ustawy) ma na celu transpozycję dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW[3] (dalej: dyrektywa 2016/680). Niniejsza opinia nie dotyczy całego projektu ustawy, lecz zawężona jest do tematyki bezpieczeństwa danych w kontekście ich gromadzenia, przechowywania, przesyłania i dostępu.

Uwagi ogólne dotyczące bezpieczeństwa danych w projekcie ustawy

Ustawowe reguły bezpieczeństwa danych osobowych nie są nowością w polskim porządku prawnym. W obowiązującej jeszcze częściowo ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2016, poz. 922) zagadnienia te uregulowane są w rozdziale 5 „Zabezpieczenie danych osobowych". Projekt ustawy reguluje te kwestie w oddziale 2 „Zabezpieczenie danych osobowych" (należącym do rozdziału 5) i zasadniczo nie wprowadza drastycznie odmiennych rozwiązań, ale precyzuje i rozszerza obowiązki w zakresie bezpieczeństwa danych. Do najważniejszych zmian należą:

- uznanie, obok administratora danych, również podmiotu przetwarzającego (tj. osoby fizycznej lub prawnej, organu władzy publicznej, jednostki organizacyjnej lub innego podmiotu, który przetwarza dane osobowe w imieniu administratora, art. 3 pkt 1 projektu ustawy), jako podmiotu zobowiązanego do zapewnienia ochrony przetwarzania danych osobowych (art. 39 projektu ustawy),
- doprecyzowanie celów zabezpieczenia danych osobowych, choć ich główne założenia pozostają bez zmian (art. 39 projektu ustawy),
- wprowadzenie procedury zgłaszania naruszeń ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych (art. 44 projektu ustawy),
- wprowadzenie procedury zawiadomienia o naruszeniu ochrony danych osobowych osób, których dane dotyczą (art. 45 projektu ustawy),

---

[2] Druk sejmowy nr 2989/VIII kad.

[3] Dz.Urz. UE L 119 z 4 maja 2018 r., s. 89.

- rezygnacja z funkcji administratora bezpieczeństwa informacji na rzecz inspektora ochrony danych (oddział 3 w rozdziale 5 projektu ustawy),
- modyfikacja obowiązku sporządzenia sprawozdania o zgodności przetwarzania danych osobowych z ustawą, które sporządzać i przekazywać administratorowi będzie inspektor ochrony danych raz na rok, do końca I kwartału za rok ubiegły (art. 47 ust. 1 pkt 9 projektu ustawy); usunięto również elementy sprawozdania (art. 36c dawnej ustawy o ochronie danych osobowych),
- ocena skutków ryzyka w przypadku, kiedy rodzaj przetwarzania danych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych administrator dokonuje apriorycznej oceny skutków planowanych operacji oraz występuje do Prezesa Urzędu Ochrony Danych Osobowych z wnioskiem o konsultacje (art. 37 i 38 projektu ustawy).

Zmiany powyższe podyktowane są koniecznością dostosowania do rozwiązań przyjętych w dyrektywie 2016/680. Rozszerzenie podmiotów zobowiązanych do zapewnienia bezpieczeństwa przetwarzania na podmiot przetwarzający wynika z art. 29 ust. 1 dyrektywy 2016/680. Artykuł 29 ust. 2 dyrektywy 2016/680 wymienia również cele zabezpieczenia danych, które powtórzone zostały w art. 39 projektu ustawy. Procedurę zgłaszania naruszeń organowi nadzorczemu[4] oraz zawiadamianie osoby, której dane dotyczą, o ich naruszeniu, regulują art. 30 i 31 dyrektywy 2016/680. Inspektor ochrony danych pojawia się w art. 32–34 dyrektywy 2016/680, stąd konieczność zmiany administratora bezpieczeństwa informacji na nowy podmiot. W tym zakresie proponowane w projekcie ustawy zmiany są zarówno uzasadnione w świetle transpozycji dyrektywy 2016/680, jak i spójne z krajowymi rozwiązaniami w zakresie ochrony danych osobowych. Ocena skutków ryzyka i obowiązek konsultacji w niektórych wypadkach wynika z art. 27 dyrektywy 2016/680. Co istotne, procedury zabezpieczania danych osobowych dotyczą zarówno środków technicznych, jak i organizacyjnych, co również znalazło się w projekcie ustawy (art. 39).

Bezpieczeństwo danych to jednak nie tylko oddział 2 projektu ustawy, ale również rozwiązania przyjęte w dyrektywie 2016/680, które ujęte zostały w innych częściach projektu. Istotna jest tutaj zwłaszcza ocena ryzyka naruszeń danych osobowych i wiążący się z tym obowiązek uwzględniania zabezpieczeń da-

[4] Zgodnie z ustawą z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000, ze zm.) organem nadzorczym, o którym mowa w rozdziale VI rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz. UE L 119 z 4 maja 2016 r., s. 1; dalej: RODO) oraz rozdziale VI dyrektywy 2016/680, jest Prezes Urzędu Ochrony Danych Osobowych.

nych w fazie projektowania oraz domyślnej ochrony danych. W art. 20 dyrektywy 2016/680 wyrażono obowiązek administratora polegający na wdrażaniu środków technicznych i organizacyjnych adekwatnych do stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia i wadze naruszeń danych osobowych m.in. w celu nadania przetwarzaniu niezbędnych zabezpieczeń zarówno w czasie określania sposobów technicznych przetwarzania, jak i w czasie samego przetwarzania. Obowiązek ten ujęty został również w art. 32 ust. 1 projektu. Dyrektywa jednak dookreśla powyższy obowiązek w art. 29 dotyczącym bezpieczeństwa przetwarzania. Wskazuje w nim, że kierując się tymi samymi przesłankami, zarówno administrator, jak i podmiot przetwarzający mają obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych dla zagwarantowania poziomu bezpieczeństwa odpowiadającego zagrożeniu, zwłaszcza jeżeli chodzi o przetwarzanie danych wrażliwych (art. 14 projektu ustawy). Konfrontując art. 29 dyrektywy 2016/680 z art. 32 i 39 projektu ustawy, wskazać należy, że choć art. 32 projektu ustawy zobowiązuje do „nadania przetwarzaniu niezbędnych zabezpieczeń", art. 29 ust. 1 dyrektywy 2016/680 jest w tym zakresie bogatszy, bowiem dotyczy „zagwarantowania poziomu bezpieczeństwa odpowiadającego zagrożeniu", wskazuje kryteria wdrażania odpowiednich środków technicznych i organizacyjnych oraz wyłącza przed nawias ochronę danych wrażliwych. Tymczasem art. 39 projektu nie wskazuje wymienionych kryteriów (stan wiedzy technicznej, koszt wdrożenia itp.), a odpowiednie stosowanie art. 32 projektu ustawy w tym zakresie nie jest wystarczające z tego względu, że przepis ten dotyczy tylko administratora, a art. 39 odnosi się również do podmiotu przetwarzającego. Z tego względu konieczne jest uzupełnienie art. 39 projektu ustawy o wskazane w art. 29 dyrektywy 2016/680 kryteria wdrażania odpowiednich środków technicznych i organizacyjnych oraz dla zagwarantowania poziomu bezpieczeństwa odpowiadającego zagrożeniu i uwzględnienie danych wrażliwych.

Konieczność uzupełnienia art. 39 projektu ustawy uzasadnia także przyjęty zarówno w dyrektywie 2016/680, jak i RODO (art. 25) model polegający na dedykowaniu decyzji o tym, co w danym kontekście stanowi odpowiednie środki techniczne i organizacyjne, administratorom danych. Celem powyższych rozwiązań jest, z jednej strony, pozostawienie administratorowi swobody w zakresie projektowania polityki bezpieczeństwa i wyboru tych środków, które w konkretnych przypadkach najlepiej zabezpieczą dane osobowe (faza projektowania), a z drugiej zapewnienie ciągłego monitorowania przez administratora stanu faktycznego i uwzględniania m.in. postępu technologicznego, który może wpłynąć na konieczność modyfikacji polityki zabezpieczenia danych (domyślna ochrona danych). Z tych względów, biorąc pod uwagę zakres swobody w ustalaniu sposobów zabezpieczenia danych, projekt ustawy słusznie nie odwołuje się do aktu wykonawczego, jakim obecnie jest rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania

danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. poz. 1024). Biorąc pod uwagę opisywaną zmianę (powierzenie administratorom decyzji o odpowiednich środkach technicznych i organizacyjnych) oraz brak szczegółowych wytycznych w tym zakresie, projekt powinien uwzględnić kryteria doboru środków, wskazanych w art. 29 dyrektywy 2016/680 (stan wiedzy technicznej i koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia), jakimi powinni się kierować administratorzy i podmioty przetwarzające, zapewniając bezpieczeństwo przetwarzania danych.

Uwagi szczegółowe

Bezpieczeństwo gromadzenia

W analizie bezpieczeństwa gromadzenia danych osobowych kluczowe są: a) proporcjonalność i podstawy gromadzenia danych; b) zakres gromadzonych danych oraz c) katalog osób upoważnionych do gromadzenia danych. Kwestie te zwiększają bowiem gwarancję tego, że dane nie będą gromadzone bez podstawy prawnej, przez nieuprawnione do tego osoby i w szerszym zakresie niż wynika to z ustawy. Kwestie te ujęte zostały w projekcie ustawy w następujących artykułach:

- art. 13 (zgodność z prawem i proporcjonalność przetwarzania),
- art. 31 ust. 1 pkt 1–4 (zgodność z prawem, rzetelność i minimalizacja przetwarzania danych oraz dbałość o jakość danych),
- art. 41 (uprawnienie do przetwarzania danych wyłącznie na podstawie upoważnienia),
- art. 19 i 20 (kategoryzacja danych pod kątem osób, których dane dotyczą, oraz jakości danych).

Wśród wymienionych wyżej przepisów gwarantujących bezpieczeństwo gromadzenia danych zastrzeżenia budzi niewykorzystany potencjał art. 19 projektu ustawy dotyczącego kategoryzacji danych pod kątem osób, których dane dotyczą. Przepis ten w aktualnym brzmieniu, poza nałożeniem na administratora i podmiot przetwarzający dodatkowych obowiązków, nie rodzi żadnych korzyści na gruncie ochrony i bezpieczeństwa danych osobowych. Poszczególne kategorie danych osobowych określone w art. 19 można jednak wykorzystać, przypisując im zakres danych, które mogą być gromadzone w odniesieniu do poszczególnych osób, co poważnie wpłynie na bezpieczeństwo gromadzenia danych poprzez minimalizację ryzyka wystąpienia sytuacji, kiedy dane osobowe pozyskane zostaną przez nieupoważnioną do tego osobę lub w zakresie szerszym niż do konieczne. Wyliczenie zakresu danych, które mogą być gro-

madzone w odniesieniu do kategorii osób, powinno znaleźć się w przedmiotowej ustawie lub ustawach dotyczących kompetencji poszczególnych organów do gromadzenia danych osobowych, a także w ustawie z 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (t.j. Dz.U. 2018, poz. 424), zwłaszcza w art. 13 dotyczącym zakresu gromadzonych danych, w którym projekt ustawy zmienia jedynie tytuł wprowadzenia do wyliczenia. Ponadto można zakładać wysokie prawdopodobieństwo wymiany danych między organami zajmującymi się zapobieganiem i zwalczaniem przestępczości. Z tego powodu sensowne byłoby ujednolicenie w przedmiotowej ustawie lub w akcie wykonawczym metodologii klasyfikacji zarówno podmiotu danych (art. 19), jak i ich jakości (art. 20).

Proponowane rozwiązanie byłoby również zgodne z zasadą minimalizacji danych wyrażoną w art. 4 ust. 1 c dyrektywy 2016/680, zgodnie z którą dane mają być adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane. Wspominając o zasadach przetwarzania danych, warto na marginesie dodać, że w rozdziale 3 projektu ustawy „Zasady przetwarzania danych osobowych" ujęto jedynie zasadę zgodności z prawem oraz rzetelności przetwarzania (art. 13). Pozostałe zasady, wyrażone w art. 4 dyrektywy 2016/680, w tym wspomniana już zasada minimalizacji, proporcjonalności, jakości i bezpieczeństwa ochrony danych, umieszczono w dalszych częściach projektu ustawy (zwłaszcza w art. 31 dotyczącym obowiązków administratora). Rozwiązanie takie marginalizuje wspomniane zasady przetwarzania, które zastosowanie mają przecież nie tylko do administratora, ale do wszystkich podmiotów przetwarzających, i może budzić wątpliwości w praktyce. Z tego powodu, choć nie jest to bezpośrednio przedmiot niniejszej opinii, należy postulować rozszerzenie rozdziału 3 projektu ustawy o pozostałe zasady przetwarzania danych, które obecnie wyrażone są w art. 31 projektu, dotyczącym obowiązków administratora.

Bezpieczeństwo przechowywania

Przy bezpieczeństwie przechowywania danych kluczowe są: a) dbałość o odpowiednie środki techniczne gwarantujące dostęp wyłącznie osobom uprawnionym, a także ochronę przed utratą, modyfikacją czy błędami systemu, b) termin przechowywania oraz c) procedura usuwania zbędnych danych. Elementy powyższe regulują następujące przepisy projektu ustawy:

- art. 39 pkt 3 (kontrola przechowywania),
- art. 39 pkt 9 (odzyskiwanie),
- art. 39 pkt 10 (integralność i niezawodność),
- art. 40 (niszczenie informatycznych nośników danych wykorzystywanych do przetwarzania danych osobowych),
- art. 31 ust. 1 pkt 5 (obowiązek administratora do przechowywania danych w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania),

- art. 31 ust. 1 pkt 6 (obowiązek zagwarantowania przez administratora bezpieczeństwa przetwarzania danych osobowych),
- art. 36 (ewidencja czynności przetwarzania zapewniająca integralność i bezpieczeństwo danych osobowych),
- art. 16 (termin przechowywania, weryfikacja i usuwanie danych zbędnych).

Przepisy te uznać należy za gwarantujące bezpieczeństwo przechowywania danych. Na negatywną ocenę zasługuje jednak w związku z tym art. 17 projektu ustawy, który dane osobowe uznane za zbędne pozwala przekształcić w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań. Przepis ten dotyczy zatem pseudonimizacji, która zgodnie z definicją zawartą w art. 3 pkt 5 dyrektywy 2016/680 oraz identyczną definicją zawartą w art. 4 pkt 16 projektu ustawy zapewnia przetworzenie danych w taki sposób, aby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi, uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

W kontekście przywołanej definicji art. 17 projektu ustawy budzi wątpliwości z powodu:

- niewystarczającego zabezpieczenia przed „odwróconą pseudonimizacją". Zawarta w ustawie definicja jest bowiem stanowcza: „aby nie można ich było już przypisać konkretnej osobie", podczas gdy w projekcie zakłada się „w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań",
- braku wyłączenia części danych (dodatkowych informacji) i osobnego ich przechowywania, a także objęcia środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie.

Konieczna wydaje się zatem modyfikacja art. 17 projektu ustawy w taki sposób, aby był on zgodny z art. 4 pkt 16 w zakresie ochrony przed odwróconą pseudonimizacją.

Bezpieczeństwo przesyłania

Przesyłanie danych, poza środkami technicznymi i organizacyjnymi opisanymi w pozostałych punktach niniejszej opinii, wymaga zagwarantowania, aby dane nieprawidłowe, niekompletne lub nieaktualnie nie były przesyłane ani udostępniane, a także, jeżeli dane wymagają szczególnych warunków przetwarzania, aby były one przestrzegane również przez odbiorcę danych. Cele te realizuje art. 21 projektu ustawy, który zobowiązuje właściwy organ do:

- weryfikacji, w miarę potrzeby i możliwości, prawidłowości, kompletności i aktualności przesyłanych danych oraz do przekazania odbiorcom niezbędnych dodatkowych informacji pozwalających odbiorcy ocenić stopień prawidłowości, kompletności i aktualności przesyłanych danych,
- niezwłocznego poinformowania odbiorcy o przesłaniu nieprawdziwych, niekompletnych lub nieaktualnych danych osobowych lub przesłania ich z naruszeniem ustawy,
- przekazania odbiorcy informacji o szczególnych warunkach przetwarzania, jeśli takie mają miejsce w odniesieniu do przesyłanych danych.

Przepis ten gwarantuje zatem jakość przesyłanych danych, o czym mowa w art. 7 dyrektywy 2016/680. Jedyną nieścisłością jest dodanie w art. 21 ust. 2 słów „w miarę potrzeby", dyrektywa bowiem posługuje się terminem „w miarę możliwości, we wszystkich przypadkach". Postuluje się zatem zmianę art. 21 ust. 2 przez usunięcie powyższego zwrotu, który zawęża obowiązek przesyłania dodatkowych informacji o jakości danych, podczas gdy dyrektywa zmierza do aktualizowania tego obowiązku we wszystkich przypadkach.

Bezpieczeństwo dostępu

Bezpieczeństwo dostępu, poza środkami technicznymi, opiera się w dużej mierze na środkach organizacyjnych przyjętych w celu zapewnienia, aby do danych osobowych dostęp miały wyłącznie osoby uprawnione i tylko w zakresie przyznanego im uprawnienia. Cele te realizują następujące przepisy projektu ustawy:

- dotyczące kontroli i ograniczania dostępu do danych:
  - art. 39 pkt 1 (kontrola dostępu do sprzętu),
  - art. 39 pkt 2 (kontrola dostępu do nośników danych),
  - art. 39 pkt 4 (kontrola użytkowników mających dostęp do danych),
  - art. 39 pkt 5 (kontrola dostępu do danych),
  - art. 39 pkt 6 (kontrola przesyłu danych, w tym informacji o dostępie),
  - art. 39 pkt 7 (kontrola wprowadzania danych),
  - art. 39 pkt 8 (ochrona przed nieuprawnionym dostępem podczas przenoszenia nośników danych),
  - art. 36 (ewidencja dostępu do danych),
- dotyczące uprawnień w zakresie dostępu do danych:
  - art. 41 (konieczność upoważnienia do przetwarzania danych osobowych oraz zapewnienia bezpieczeństwa przetwarzania),
  - art. 42 (ewidencja osób upoważnionych oraz zakres upoważnienia),
  - art. 43 (obowiązki osób upoważnionych w związku z upoważnieniem do przetwarzania danych),
- dotyczące zakresu dostępu do przetwarzania danych:
  - art. 41 (nadanie upoważnienia do przetwarzania w ramach danej kategorii).

Gwarancje bezpieczeństwa danych są zatem skrupulatnie wymienione w projekcie ustawy, niemniej brakuje w nim kilku ważnych elementów. Po pierwsze, w art. 41 projektu ustawy zbyt wąsko określono zakres dostępu do przetwarzania danych, ograniczając go tylko do kategorii czynności przetwarzania. Rozwiązanie to jest niedoskonałe z tego względu, że nie uwzględnia kategorii osób i rodzaju danych, do których uzyskuje się dostęp. Istotne bowiem jest nie tylko to, jakie operacje osoba uprawniona może wykonywać, ale przede wszystkim, do jakich danych może mieć dostęp. Ponownie, narzucona przez dyrektywę i ujęta w art. 19 projektu ustawy, kategoryzacja może okazać się rozwiązaniem pomocnym w określeniu w upoważnieniach nie tylko czynności przetwarzania, ale również zakresu danych, do których konkretne osoby mogą mieć dostęp. Po drugie, w projekcie zabrakło gwarancji związanych z dostępem do danych, o których mowa w art. 14 projektu („dane wrażliwe"). I w tym wypadku postuluje się zwiększone środki bezpieczeństwa, tj. konieczność uzyskania indywidualnego upoważnienia do przetwarzania tego rodzaju danych. Po trzecie, upoważnienie do przetwarzania danych, o którym mowa w art. 41 projektu ustawy, powinno być nadawane wyłącznie przez administratora lub inspektora, a nie przez podmiot przetwarzający, którego zadaniem nie jest kontrola dostępu do danych osobowych. Obecne rozwiązanie budzi wątpliwości w zakresie wystarczającej ochrony przed nieuprawnionym dostępem, spójności z przepisami dotyczącymi ewidencji osób upoważnionych do przetwarzania (art. 42 projektu ustawy) oraz kontroli bezpieczeństwa dostępu do danych.

Ponadto, w celu zwiększenia świadomości obowiązków wynikających z uzyskania dostępu do przetwarzania danych i zminimalizowania wiążącego się z tym ryzyka naruszeń, osoba upoważniona przed uzyskaniem dostępu do danych powinna zostać poinformowana o obowiązkach, o których mowa w art. 43 projektu ustawy.

Wnioski

- Większość rozwiązań zaproponowanych w projekcie ustawy dotyczących bezpieczeństwa gromadzenia, przechowywania, przesyłania i dostępu do danych osobowych daje wysoką gwarancję bezpieczeństwa danych oraz jest zgodna ze standardami dyrektywy 2016/680 (art. 39–45, art. 31–32, art. 13, art. 19, art. 20, art. 21).
- W wielu miejscach opiniowany projekt zawiera jednak rozwiązania, które nie gwarantują bezpieczeństwa danych osobowych.
- Artykuł 39 projektu ustawy nie zawiera wskazanych w art. 29 dyrektywy 2016/680 kryteriów wdrażania odpowiednich środków technicznych i organizacyjnych dla zagwarantowania poziomu bezpieczeństwa danych osobowych odpowiadającego zagrożeniu oraz uwzględniania w tym kontekście danych

wrażliwych, przez co administrator i podmiot przetwarzający pozbawieni są wytycznych w projektowaniu środków technicznych i organizacyjnych bezpieczeństwa danych.

▪ Zwiększenie bezpieczeństwa gromadzenia danych jest możliwe przez wyliczenie w projekcie ustawy lub ustawach szczególnych oraz w ustawie z 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych rodzajów danych, jakie mogą być gromadzone w odniesieniu do poszczególnych kategorii osób, o których mowa w art. 19 projektu. Ponadto, ze względu na wysokie prawdopodobieństwo wymiany danych pomiędzy organami zajmującymi się zapobieganiem i zwalczaniem przestępczości, sensowne byłoby ujednolicenie w przedmiotowej ustawie lub w akcie wykonawczym metodologii klasyfikacji zarówno podmiotu danych (art. 19), jak i ich jakości (art. 20).

▪ Zagrożeniem dla bezpieczeństwa przechowywania danych osobowych jest art. 17 projektu ustawy, który nie jest zgodny z art. 4 pkt 16 w zakresie ochrony przed odwróconą pseudonimizacją.

▪ W celu wzmocnienia bezpieczeństwa przesyłania danych postuluje się zmianę art. 21 ust. 2 przez wprowadzenie obowiązku przesyłania dodatkowych informacji o jakości danych we wszystkich przypadkach, a nie, jak dotychczas, „w miarę potrzeby".

▪ Projekt zawiera istotne luki w zakresie bezpieczeństwa dostępu do danych:

– w art. 41 projektu ustawy zbyt wąsko określono zakres dostępu do przetwarzania danych, ograniczając go tylko do kategorii czynności przetwarzania z pominięciem kategorii osób i rodzaju danych, do których uzyskuje się dostęp. Rozwiązaniem tego problemu może być odwoływanie się w upoważnieniu do kategoryzacji danych, o której mowa w art. 19 projektu ustawy,
– w projekcie zabrakło gwarancji związanych z dostępem do danych, o których mowa w art. 14 projektu („dane wrażliwe"). Może to być np. konieczność uzyskania indywidualnego upoważnienia do przetwarzania tego rodzaju danych,
– upoważnienie do przetwarzania danych, o którym mowa w art. 41 projektu ustawy, powinno być nadawane wyłącznie przez administratora lub inspektora, a nie przez podmiot przetwarzający, którego zadaniem nie jest kontrola dostępu do danych osobowych,
– w celu zwiększenia świadomości obowiązków wynikających z uzyskania dostępu do przetwarzania danych i zminimalizowania wiążącego się z tym ryzyka naruszeń osoba upoważniona przed uzyskaniem dostępu do danych powinna zostać poinformowana o obowiązkach, o których mowa w art. 43 projektu ustawy.