https://doi.org/10.31268/ZPBAS.2018.66 nr 4(60) 2018 ▪ s. 95–107 ZESZYTY PRAWNICZE BAS Biura Analiz Sejmowych Kancelarii Sejmu

Grzegorz Sibiga

Ocena rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy nr 2989)[1]

Assessment of the governmental Bill on the Protection of Personal Data Processed in Relation to the Prevention of and Fighting Crime (Sejm's Paper no. 2989): The provisions of the bill indicated in the opinion raise doubts from the in terms of their compliance with the directive and complementarity with the Regulation of the European Parliament and of the Council (EU) 2016/679. Among others the adoption of the act in the designed form will result in the fact that, within a specified time, the obliged entities will not be able to apply any of the basic security principles specified in the act, what creates a risk for the actual data security. The project disperses regulations regarding the security of personal data in many normative acts. There are no sanctions for breach of personal data security obligations, what may be considered as a lack of implementation of the requirement set out in the Directive.

Keywords: personal data protection, bill, crime, European Union
Słowa kluczowe: ochrona danych osobowych, projekt ustawy, przestępczość, Unia Europejska

Doktor nauk prawnych, Instytut Nauk Prawnych Polskiej Akademii Nauk ▪ gsibiga@inp.pan.pl ▪ https://orcid.org/0000-0002-4721-8272

Przedmiot opinii

Przedmiotem opinii jest ocena rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy nr 2989/VIII kad.) pod kątem bezpieczeństwa gromadzenia, przechowywania, przesyłania i dostępu do danych osobowych.

[1] *Opinia prawna dotycząca rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk sejmowy nr 2989)* sporządzona 30 listopada 2018 r. na zlecenie Biura Analiz Sejmowych; BAS 2768/18.

Ocena projektu ustawy

Kryteria oceny

W niniejszej opinii przyjęto cztery kryteria oceny projektu ustawy.

- **Poprawność implementacji dyrektywy 2016/680**

Celem omawianego projektu ustawy jest implementacja do krajowego porządku prawnego 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 uchylająca decyzję ramową Rady 2008/977/WSiSW[2]. Zgodnie z definicją zamieszczoną w art. 288 TFUE dyrektywa, podobnie jak rozporządzenie czy decyzja, jest wiążącym aktem prawnym. Dyrektywa jest tym rodzajem aktu, który wiąże w odniesieniu do rezultatu, który ma być osiągnięty przez państwa członkowskie, będące jej adresatami, ale pozostawia organom tych państw swobodę wyboru formy i środków.

- **Komplementarność z RODO oraz z ustawami krajowymi uzupełniającymi RODO**

Na pakiet reformujący ochronę danych osobowych w UE składają się dyrektywa 2016/680 oraz rozporządzenie PE 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 (ogólne rozporządzenie o ochronie danych)[3]. Dyrektywa 2016/680 traktowana jest jako uzupełnienie RODO w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. W tym zakresie RODO bowiem wyłącza stosowanie swoich przepisów (tak art. 2 ust. 2 lit. d RODO), ponieważ jest to objęte zakresem dyrektywy 2016/680 (art. 1 ust. 1 dyrektywy). Jednak sam projektodawca w uzasadnieniu projektu słusznie wskazuje, że oba akty w sposób spójny i kompleksowy regulują zagadnienia ochrony danych[4]. Takie stwierdzenie jest uzasadnione, ponieważ znaczna część rozwiązań

---

[2] Dz.Urz. UE L 119 z 4 maja 2016 r., s. 89; dalej: dyrektywa 2016/680.

[3] Dz.Urz. UE L 119 z 4 maja 2016 r., s. 1; dalej: RODO.

[4] Uzasadnienie. Rządowy projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, druk sejmowy nr 2989/VIII kad., s. 1; dalej: uzasadnienie.

uregulowanych w dyrektywie 2016/680 pozostaje zbieżna z rozwiązaniami przyjętymi w RODO i dlatego wymagają one jednolitego stosowania.

Przepisy RODO, w zakresie dopuszczonym w samym RODO, muszą lub mogą być uzupełniane przepisami prawa krajowego. Podstawowym aktem krajowym uzupełniającym RODO, przede wszystkim w zakresie przepisów proceduralnych oraz ustrojowych, jest ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000, ze zm.). Na potrzebę komplementarności rozwiązań obu aktów (projektu ustawy oraz ustawy o ochronie danych osobowych z 2018 r.) wskazują liczne odesłania zawarte w projekcie ustawy do ustawy o ochronie danych osobowych uchwalonej 10 maja 2018 r.

■ **Zapewnienie wysokiego stopnia ochrony danych osobowych**

Jednym z podstawowych celów dyrektywy 2016/680 jest zapewnienie wysokiego stopnia ochrony danych osobowych (motywy 4 i 7 dyrektywy), co ma nastąpić m.in. poprzez wzmocnienie praw osób, których dane dotyczą, oraz obowiązki podmiotów, które dane osobowe przetwarzają (motyw 7 dyrektywy 2016/680). Również w uzasadnieniu ustawy powtarza się argument o konieczności zapewnienia spójnego, wysokiego stopnia ochrony danych osobowych osób fizycznych (uzasadnienie, s. 2). Dlatego też zasadne jest ocenianie przepisów projektowanej ustawy z punktu widzenia celu reformy przepisów o ochronie danych osobowych.

■ **Ocena z punktu widzenia regulacji zastępowanej.**

Przepisy projektowanej ustawy zastąpią w porządku krajowym przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2016, poz. 922, ze zm.). Do przetwarzania danych osobowych objętych zakresem projektu ustawy zastosowanie znajdują przepisy ustawy z 1997 r.: do 25 maja 2018 r. na mocy samej ustawy z 1997 r. (zob. art. 2 tej ustawy), natomiast od 25 maja 2018 r. na podstawie art. 175 nowej ustawy o ochronie danych osobowych z 2018 r., z wyjątkami określonymi w tym przepisie. Ponieważ celem projektu ustawy jest zapewnienie wysokiego stopnia ochrony danych osobowych, to w ocenie autora projektowana ustawa nie powinna obniżać poziomu ochrony danych w stosunku do ustawy z 1997 r.

Wyłączenia spod mocy ustawy

Istotny wpływ na zasady bezpieczeństwa danych osobowych ma zakres stosowania przepisów o ochronie danych osobowych, w tym też całościowe wyłączenia spod mocy projektowanej ustawy. Konsekwencją zastosowania takiego wyłączenia jest bowiem niestosowanie wszystkich analizowanych w dalszej części opinii przepisów dotyczących środków zabezpieczających dane osobowe. W przypadku przedmiotowego projektu ustawy ma to istotne konsekwencje, ponieważ projekt przewiduje znaczne wyłączenia spod mocy ustawy określone w art. 3 pkt 1 i pkt 2 oraz w zmienianej w art. 84 projektu ustawie o ochronie informacji nie-

jawnych. Najszersze zdaje się wyłączenie zawarte w art. 3 pkt 1 projektu ustawy, zgodnie z którym: *przepisów ustawy nie stosuje się do ochrony danych osobowych znajdujących się w aktach spraw lub czynności lub urządzeniach ewidencyjnych, w tym tworzonych i przetwarzanych z wykorzystaniem technik informatycznych*, prowadzonych na podstawie wymienionych w projekcie ustaw procesowych.

W uzasadnieniu projektodawca tłumaczy to wyłączenie trzema rodzajami argumentów: 1) nieprzetwarzaniem w tych sytuacjach danych osobowych w zbiorze danych, co stanowi warunek objęcia zakresem stosowania dyrektywy 2016/680 (art. 2 ust. 2 dyrektywy); (uzasadnienie, s. 9), 2) dopuszczeniem w art. 18 dyrektywy 2016/680 oraz w motywach 20 i 49 wprowadzenia odmiennego reżimu w prawie krajowym dla przetwarzania danych osobowych w postępowaniu karnym(uzasadnienie, s. 12), 3) potrzebą „ostrożności" w regulacji uprawnień związanych z ochroną danych osobowych w postępowaniu karnym, ze względu na konieczność zachowania proporcji między prawem do ochrony danych osobowych oraz innymi prawami realizowanymi w postępowaniu karnym (uzasadnienie, s. 12).

Wyłączenie zawarte w art. 3 pkt 1 projektu ustawy, z powołaniem się w uzasadnieniu projektu na brak funkcjonowania zbioru danych w przypadku przetwarzania danych osobowych w urządzeniach ewidencyjnych oraz w systemie teleinformatycznym, nie może się ostać z punktu widzenia zgodności z art. 2 ust. 2 dyrektywy 2016/680 wyznaczającym jej zakres stosowania. Projektodawca w uzasadnieniu wskazuje, że kryterium zastosowania dyrektywy jest funkcjonowanie zbioru danych, co tylko częściowo pokrywa się z brzmieniem wspomnianego przepisu dyrektywy. Przepis art. 2 ust. 2 stanowi, że: *niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany, oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych*.

Zakres ten należy odnieść do trzech użytych w art. 3 pkt 1 projektu ustawy pojęć dotyczących organizacji przetwarzania danych osobowych: akta sprawy, urządzenie ewidencyjne oraz technika informatyczna. Cechą każdego urządzenia ewidencyjnego, ze względu na zakres znaczeniowy tego zwrotu, jest porządkowanie danych, tak aby były one dostępne według określonych kryteriów, co spełnia przesłanki definicji zbioru danych z art. 3 pkt 5 dyrektywy 2016/680. Natomiast na mocy art. 2 ust. 2 dyrektywy 2016/680 każde przetwarzanie danych osobowych w systemie informatycznym lub teleinformatycznym, a tylko w takich systemach może zostać zastosowana technika informatyczna, będzie objęte zakresem dyrektywy, ponieważ mieści się ono w pojęciu zautomatyzowanego przetwarzania danych. Do takiego przetwarzania nie stosuje się kryterium zbioru danych, ponieważ to kryterium odnosi się tylko do przetwarzania danych w inny sposób niż zautomatyzowany. Gdy chodzi o wyodrębnione akta sprawy, to faktycznie może być dyskusyjne, czy mamy do czynienia z przetwarzaniem

danych w zbiorze, chociaż zdaniem autora opinii wystarczające dla zaistnienia zbioru jest występowanie jakiegokolwiek kryterium porządkującego akta, które pozwoli na dostęp do danych osobowych określonej osoby. Jeśli akta są połączone z systemem ewidencyjnym zapewniającym dostęp do danych osobowych zawartych w aktach sprawy dotyczących jakiejkolwiek osoby (np. uczestnika postępowania), to takie dane osobowe znajdujące się w aktach stanowią co najmniej część zbioru.

Z kolei powoływany w uzasadnieniu projektu art. 18 dyrektywy 2016/680 nie daje podstaw do całościowego wyłączenia stosowania dyrektywy, ponieważ stanowi on jedynie o możliwości kształtowania realizacji niektórych określonych w dyrektywie praw osób, których dane dotyczą (chodzi o uprawnienia wskazane w art. 13, 14 i 16 dyrektywy) zgodnie z przepisami krajowymi w postępowaniu przygotowawczym lub sądowym w sprawie karnej. W szczególności w art. 18 dyrektywy nie wymieniono żadnego z przepisów dyrektywy dotyczącego bezpieczeństwa danych osobowych. Należy zwrócić też uwagę, że posłużenie się w art. 18, tak zresztą jak w motywie 20, zwrotem „akta sprawy" świadczy o tym, że przetwarzanie w nich danych osobowych może mieścić się w zakresie stosowania dyrektywy 2016/680, a prawodawca unijny jedynie punktowo stwarza możliwość wyłączenia lub modyfikacji stosowania przepisów dyrektywy w tym względzie.

Również motywy 20 i 49 nie odnoszą się do zagadnień bezpieczeństwa danych osobowych. Celem wyrażonym w motywie 20 jest uniknięcie kolizji między przepisami dyrektywy 2016/680 oraz określanymi w krajowym prawie karnym procesowym „operacjami i procedurami przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości". W przypadku zasad bezpieczeństwa danych osobowych taka systemowa kolizja z reguły nie zaistnieje, ponieważ przedmiotem prawa karnego procesowego nie jest ustalanie obowiązków w zakresie zabezpieczania danych osobowych. Z kolei motyw 49 dotyczy tylko realizacji określonych praw osoby, której dane dotyczą w postępowaniu przygotowawczym oraz sądowym w sprawie karnej, co powinno następować zgodnie z przepisami krajowymi.

Należy więc stwierdzić, że w dyrektywie 2016/680 nie występują podstawy do wyłączania stosowania przepisów o bezpieczeństwie danych osobowych w zakresie wskazanym w art. 3 pkt 1 projektu ustawy, w sytuacji gdy to przetwarzanie następuje w granicach wyznaczonych w art. 2 dyrektywy 2016/680.

Przepisy o zabezpieczeniu danych osobowych

Problematyka środków technicznych i organizacyjnych zabezpieczających dane osobowe jest regulowana w dyrektywie 2016/680 w różnych jej przepisach, przede wszystkich w zasadzie zawartej w art. 19 oraz w rozdziale IV, a głównie w sekcji 2 tego rozdziału. Jednak również inne obowiązki określone w dyrektywie należy oceniać pod kątem zastosowania odpowiednich środków technicznych i organi-

zacyjnych wspomagających ich wykonanie, np. obowiązki dotyczące przechowywania danych osobowych są związane z technicznymi i organizacyjnymi aspektami usuwania danych po upłynięciu okresów dopuszczalnego przechowywania.

Do przepisów projektu ustawy w tym względzie należy zgłosić uwagi mające charakter:

- uwag generalnych, dotyczących samego sposobu podejścia projektodawcy do wdrożenia w porządku krajowym wymagań określonych w dyrektywie 2016/680,
- uwag szczegółowych do konkretnych rozwiązań przyjętych w projekcie ustawy.

■ Uwagi generalne

Zdaniem autora opinii istnieją dwa problemy generalne.

- Wprowadzenie dodatkowych okresów dostosowawczych na wdrożenie środków technicznych i organizacyjnych zabezpieczających dane osobowe.
- Ogólny charakter rozwiązań przewidzianych w ustawie głównej połączony z przeniesieniem do zmienianych odrębnych ustaw określenia szczegółowych środków zabezpieczających (problem rozproszenia zasad bezpieczeństwa danych osobowych w wielu aktach prawnych).

- *Ad*. 1. Dodatkowe terminy dostosowawcze

Projekt ustawy przewiduje dwa terminy dostosowawcze dla adresatów obowiązków na wdrożenie wymaganych środków technicznych i organizacyjnych:

- jednego roku od dnia wejście w życie ustawy na wdrożenie podstawowych zasad bezpieczeństwa danych określonych w art. 39 projektu (art. 103 ust. 1 projektu),
- do 6 maja 2023 r. na dostosowanie zautomatyzowanych systemów przetwarzania danych osobowych do środków technicznych i organizacyjnych przewidzianych w ustawie, jeżeli to dostosowanie wymaga niewspółmiernie dużego wysiłku lub nakładów (art. 103 ust. 2 projektu).

Obydwa wyżej wymienione okresy dostosowawcze zostały przewidziane bez uwzględnienia wymogów co do transpozycji przepisów określonych w art. 63 dyrektywy 2016/680. Dyrektywa w art. 63 ust. 3 dopuszcza w drodze wyjątku, że państwo członkowskie może wprowadzić okres dostosowawczy do 6 maja 2023 r. dla zautomatyzowanych systemów przetwarzania, jeżeli wymagałoby to niewspółmiernie dużego wysiłku, ale okres ten może dotyczyć wyłącznie systemów utworzonych przed dniem 6 maja 2016 r. Tymczasem w art. 103 ust. 2 projektu ustawy nie wskazuje się, jakich zautomatyzowanych systemów dotyczy ten przepis, co oznacza, że może on obejmować wszystkie takie systemy, tj. systemy istniejące w dniu wejścia w życie przyjmowanej ustawy, ale również systemy tworzone później.

Natomiast dyrektywa w ogóle nie dopuszcza możliwości wprowadzenia okresu dostosowawczego, o którym mowa w art. 103 ust. 1 projektu. Zgodnie z art. 63 ust. 1 dyrektywy 2016/680 państwa członkowskie miały przyjąć i opublikować do 6 maja 2018 r. przepisy niezbędne do wykonania niniejszej dyrektywy. Również od 6 maja 2018 r. państwa członkowskie miały obowiązek stosowania tych przepisów (art. 63 ust. 1 zdanie trzecie). Od dnia 25 maja 2018 r. na podstawie art. 175 ustawy z 10 maja 2018 r. o ochronie danych osobowych pozostawiono w mocy wskazane przepisy dotychczasowej ustawy o ochronie danych osobowych z 1997 r. w stosunku do przetwarzania danych osobowych objętych zakresem dyrektywy 2016/680. Przepisy te będą obowiązywały w okresie do dnia wejścia w życie ustawy wdrażającej przedmiotową dyrektywę. To rozwiązanie dotyczy również – odnoszących się do zabezpieczenia danych osobowych – przepisów rozdziału 5 ustawy z 1997 r. (art. 36–39a tej ustawy), które będą obowiązywały aż do wejścia w życie ustawy stanowiącej przedmiot niniejszej opinii. Z kolei według art. 108 projektu ustawy z momentem wejścia w życie tej ustawy tracą moc zachowane przepisy ustawy z 1997 r. (w tym przepisy rozdziału 5), a jednocześnie na wdrożenie przez zobowiązanych nowych zasad bezpieczeństwa danych przewidziano kolejny rok.

Oznacza to, że między dniem wejścia w życie ustawy a dniem, w którym minie rok od tego dnia, podmioty zobowiązane mogą w zgodzie z ustawą nie stosować żadnych z podstawowych zasad bezpieczeństwa, ani wskazanych w art. 39 projektu ustawy (trwa bowiem okres dostosowawczy), ani określonych w ustawie z 1997 r. (ustawa implementująca dyrektywę uchyliła ich stosowanie). W sposób oczywisty rodzi się ryzyko dla faktycznego bezpieczeństwa danych.

- *Ad*. 2. Generalny charakter rozwiązań w ustawie głównej oraz rozproszenie zasad bezpieczeństwa danych osobowych w różnych aktach normatywnych

Podstawowe reguły bezpieczeństwa danych osobowych zostały określone w zasadzie zawartej w art. 31 ust. 1 pkt 1 oraz w art. 39 projektu ustawy. Do drugiego z tych przepisów przeniesiono, pod względem językowym niezwykle dokładnie, treść art. 29 ust. 2 dyrektywy 2016/680. Nie zwrócono jednak uwagi na to, że ten przepis dyrektywy dotyczy jedynie zautomatyzowanego przetwarzania danych, ponieważ w projekcie ustawy odniesiono go do każdego rodzaju przetwarzania. W projekcie ustawy odpowiednikiem generalnej zasady doboru zabezpieczeń określonej w art. 29 ust. 1 dyrektywy jest art. 31 ust. 1 pkt 1, który uzależnia zastosowanie środków zabezpieczających od charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych (podejście oparte na ryzyku).

Należy jednak zwrócić uwagę, że art. 29 ust. 2 dyrektywy 2016/680 określa cele (rezultaty) do zrealizowania w zakresie bezpieczeństwa danych osobowych, zaś rolą państwa członkowskiego jest ustalenie, jakimi środkami rezultat ten ma być osiągnięty. Tymczasem w projekcie ustawy ograniczono się tylko do powtórzenia

za dyrektywą celów w obszarze bezpieczeństwa danych, co oznacza, że w praktyce obowiązek określenia środków, jakimi mają być one zrealizowane, został przeniesiony na adresata obowiązku (administratora lub podmiot przetwarzający). Pomimo że w kwestiach doboru zabezpieczeń danych osobowych w art. 29 ust. 1 dyrektywy 2016/680 (podobnie jak w art. 32 RODO) zostało przyjęte podejście oparte na ryzyku, co wyklucza zobowiązanie do zastosowania takich samych środków zabezpieczających przez wszystkich adresatów przepisów, to jednak, zdaniem autora niniejszej opinii, nie wyłącza to możliwości wskazania w prawie krajowym katalogu procesów służących bezpieczeństwu czy nawet środków, spośród których administrator (adresat obowiązków) może dobierać opcjonalnie zabezpieczenia po dokonanej analizie ryzyka. Za postulatem wprowadzenia takiej regulacji przemawia bardziej rozbudowany w stosunku do art. 32 RODO zakres obowiązków bezpieczeństwa określonych w art. 29 ust. 2 dyrektywy 2016/680 oraz odniesienie ich do wszystkich sytuacji zautomatyzowanego przetwarzania danych osobowych, a nie tylko do „stosownych przypadków" jak w art. 32 RODO.

Jedyne szczegółowe środki zabezpieczające zostały określone w art. 40 (niszczenie nośników danych) oraz w art. 41–43 projektu (dopuszczenie do przetwarzania danych osób upoważnionych oraz obowiązki z tym związane). Co istotne, w projekcie ustawy nie zdecydowano się na przejęcie uregulowanej w art. 53 ust. 1 pkt 4 oraz ust. 2–3 ustawy z 10 maja 2018 r. o ochronie danych osobowych instytucji rekomendacji Prezesa UODO określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych w danym rodzaju działalności. Instytucja ta ma na celu wsparcie organu nadzorczego w ustalaniu konkretnych środków zabezpieczających dla określonych rodzajów podmiotów.

Z tak generalnym określeniem zasad bezpieczeństwa w projekcie ustawy kontrastuje szczegółowe wskazywanie środków zabezpieczających do zastosowania w części ustaw nowelizowanych w rozdziale 9 („Przepisy zmieniające") projektu ustawy. Przykładowo w odrębnych ustawach określono:

- środki zabezpieczenia technicznego przy udostępnianiu danych osobowych za pomocą urządzeń służących do teletransmisji danych (art. 57 pkt 1 projektu ustawy dodający art. 22a ust. 6 w ustawie o rybactwie śródlądowym; art. 58 pkt 5 lit. b projektu ustawy dodający art. 20 ust. 1e w ustawie o Policji; art. 59 pkt 4 dodający art. 10a ust. 9 w ustawie o Straży Granicznej; art. 72 pkt 2 projektu ustawy zmieniający art. 29 ust. 5 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych; art. 82 pkt 5 projektu ustawy dodający art. 25d ust. 1 w ustawie o Służbie Więziennej),
- zabezpieczenie utrwalonego i przechowywanego obrazu i dźwięku (art. 58 pkt 4 projektu ustawy dodający art. 15b ust. 2 w ustawie o Policji),
- zasady organizacyjne usuwania danych osobowych (pkt 12 i pkt 14 w art. 58 projektu ustawy dodające odpowiednio art. 21e ust. 5 oraz art. 21n w ustawie o Policji),

- zasady organizacyjne likwidowania zbiorów danych (art. 72 pkt 2 projektu ustawy zmieniający art. 29 ust. 10 i 11 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych),
- zasady organizacyjne dopuszczenia do przetwarzania danych osobowych (upoważnianie) oraz obowiązki osób upoważnionych (art. 59 pkt 8 projektu ustawy dodający art. 50b ust. 2 w ustawie o Straży Granicznej),
- zasady organizacyjne nadawania upoważnień do przetwarzania danych osobowych (art. 72 pkt 2 projektu ustawy zmieniający art. 29 ust. 8 i 9 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych).

Dodatkowo w niektórych projektowanych ustawach przewidziano upoważnienia ustawowe dla wydania rozporządzeń określających sposoby i tryb udostępniania danych osobowych (m.in. w systemie teleinformatycznym), przy czym w ustawowych wytycznych wymaga się uwzględnienia w tych aktach zasad bezpieczeństwa udostępnianych danych (np. zob. art. 82 pkt 5 projektu ustawy dodający art. 25 ust. 2 pkt 3 w związku z ust. 1 w ustawie o Służbie Więziennej czy art. 81 pkt 13 projektu ustawy zmieniający art. 42 ust. 6 w ustawie o bezpieczeństwie imprez masowych). Tworzy się więc ustawowe podstawy do wydawania kolejnych aktów normatywnych (rozporządzeń), które mogą przewidywać następne środki zabezpieczające dane osobowe.

Powyższy sposób ustawowego unormowania stosowania środków zabezpieczających dane osobowe prowadzi do rozproszenia regulacji w tym względzie w wielu aktach normatywnych. To z kolei powoduje negatywne konsekwencje polegające na niejednolitości stosowanych prawnych zasad bezpieczeństwa w zakresie przetwarzania danych objętych dyrektywą 2016/680 przez poszczególne podmioty oraz na potrzebie równoległego stosowania przepisów dotyczących zabezpieczeń znajdujących się w co najmniej dwóch aktach prawnych, tj. w ustawie o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości (w „ustawie głównej") oraz w odrębnych ustawach lub rozporządzeniach. W tym drugim wypadku może to rodzić potrzebę rekonstruowania przez interpretatora normy prawnej dotyczącej bezpieczeństwa danych osobowych na podstawie kilka aktów prawnych, ponieważ zabezpieczanie danych stanowi tylko jeden ciąg czynności faktycznych, bez względu na liczbę aktów prawnych go regulujących. W tym kontekście wydaje się, że ustawa implementująca dyrektywę 2016/680 („ustawa główna") powinna – co do zasady – tworzyć jednolitą prawną regulację dotyczącą zabezpieczeń danych osobowych, realizującą cele określone w art. 29 tejże dyrektywy. Każda odmienność w stosunku do powyższych reguł powinna być uzasadnionym wyjątkiem (np. szczególnym ryzykiem dla praw osób, których dane dotyczą), ale jednocześnie winna być wkomponowana w uniwersalne zasady bezpieczeństwa określone w ustawie głównej. W uzasadnieniu projektu ustawy żadne ze szczegółowych rozwiązań dotyczących bezpieczeństwa nie zostało wyjaśnione.

▪ Uwagi szczegółowe

Oprócz uwag generalnych należy przedstawić kilka uwag szczegółowych do przyjętych rozwiązań dotyczących bezpieczeństwa danych osobowych.

▪ Wybór właściwego podmiotu przetwarzającego

Projekt ustawy nie wdraża podstawowego obowiązku administratora przy powierzaniu przetwarzania danych osobowych, który został określony w art. 22 ust. 1 dyrektywy 2016/680 (podobnie w art. 28 ust. 1 RODO). Istota tego obowiązku polega na tym, że dla legalnego powierzenia przetwarzania danych osobowych nie jest wystarczające samo zawarcie umowy powierzenia przetwarzania danych osobowych między administratorem oraz podmiotem przetwarzającym, tak jak było to w poprzednim stanie prawnym (zob. art. 31 ust. 1–2 ustawy o ochronie danych osobowych z 1997 r.). Według wspomnianego przepisu dyrektywy administrator może bowiem korzystać z usług wyłącznie takiego podmiotu przetwarzającego, który daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. W praktyce powoduje to dodatkowy obowiązek administratora danych – oprócz zawarcia umowy – weryfikacji podmiotu przetwarzającego pod kątem spełnienia przez niego wymogów określonych w art. 22 ust. 1 dyrektywy 2016/680. Tymczasem projekt ustawy ogranicza obowiązki administratora jedynie do zawarcia z podmiotem przetwarzającym umowy o określonej treści.

▪ Dokumentowanie naruszeń ochrony danych

Przepis art. 44 ust. 6 projektu ustawy nakazuje administratorowi dokumentowanie przypadków naruszenia ochrony danych, ale czyni to z odesłaniem do ust. 1 w tym artykule. Z kolei art. 44 ust. 1 projektu ustawy określa tylko sytuację naruszeń ochrony danych wymagających zgłoszenia do Prezesa UODO. W związku z tym na gruncie projektu dopuszczalne jest stanowisko, że obowiązek wewnętrznego dokumentowania dotyczy wyłącznie tych naruszeń. Tymczasem dyrektywa 2016/680 w art. 30 ust. 5 (podobnie w art. 33 ust. 5 RODO) wymaga, aby administrator dokumentował wszelkie naruszenia ochrony danych, tzn. niezależnie od tego, czy podlegają one obowiązkowi zgłoszenia do organu nadzorczego. W związku z tym uzasadnione pozostaje jednoznaczne wskazanie w art. 44 ust. 6 projektu, że dokumentowanie dotyczy każdego przypadku naruszenia ochrony danych.

▪ Inspektor ochrony danych

W art. 11 projektu ustawy przewiduje się, że Prezes UODO może w sposób władczy zwrócić się do inspektora ochrony danych (IOD), wyznaczonego przez administratora w swojej jednostce organizacyjnej, o przeprowadzenie dla niego sprawdzenia (audytu) w tejże jednostce, a następnie przesłanie do organu sprawozdania po sprawdzeniu. Stanowi to powtórzenie rozwiązania przewidzianego

w art. 19b ustawy o ochronie danych osobowych z 1997 r. dotyczącego relacji GIODO oraz administratora bezpieczeństwa informacji (ABI). Powyższa kompetencja może zostać zakwalifikowana jako co najmniej zbliżona do kompetencji kontrolnej. Natomiast należy zwrócić, że dyrektywa 2016/680 nie ustanawia władczych kompetencji Prezesa UODO wobec IOD, ale dla stosunku między nimi używa zwrotów „współpraca" (art. 34 lit. d), „pełnienie funkcji punktu kontaktowego" i „prowadzenie konsultacji" (art. 34 lit. e). Dyrektywa bliżej nie wyjaśnia tych pojęć, ale ich zakres znaczeniowy zdaje się wyłączać możliwość władczego oddziaływania Prezesa UODO wobec IOD, takiego jakie miało miejsce na gruncie ustawy z 1997 r. w stosunkach GIODO–ABI.

- Zasada rozliczalności

Jedną z podstawowych zasad dyrektywy 2016/680 jest określona w art. 4 ust. 4, a w przypadku środków technicznych i organizacyjnych uszczegółowiona w art. 19 ust. 1 dyrektywy, zasada rozliczalności (podobnie w art. 5 ust. 2 oraz w art. 24 ust. 1 RODO). Polega ona na tym, że to administrator (główny adresat obowiązków) musi być w stanie wykazać, że przetwarzanie przez niego danych osobowych następuje zgodnie z przepisami, co odnosi się także do zastosowanych przez niego środków technicznych i organizacyjnych. Powyższa zasada nie została przeniesiona bezpośrednio do projektu ustawy, mimo że zawarto ją w aż dwóch wyżej wskazanych przepisach dyrektywy. Inaczej niż twierdzi się w uzasadnieniu projektu (uzasadnienie, s. 26), transpozycją tej zasady do polskiego porządku prawnego nie jest art. 35 projektu ustawy, który nakazuje prowadzenie wykazu kategorii czynności przetwarzania. Według art. 24 dyrektywy 2016/680 prowadzenie wykazu to obowiązek odrębny od zasady rozliczalności, aczkolwiek także mający wpływ na jej realizację.

Występują także wątpliwości, czy za prawidłową transpozycję tej zasady można uznać przewidziane w art. 31 ust. 3 i 4 projektu ustawy obowiązki prowadzenia przez administratora dokumentacji realizacji czynności oraz polityki ochrony danych. Powyższe obowiązki stanowią bowiem sposób wykonania zasady rozliczalności, zaś sama zasada ma dużo szersze znaczenie dla określenia odpowiedzialności administratora oraz ciężaru dowodu w poszczególnych sprawach.

- **Sankcje za naruszenie przepisów**

W art. 57 dyrektywy 2016/680 wymaga się, aby państwa członkowskie przyjęły przepisy określające sankcje za naruszenie przepisów ustanowionych na podstawie niniejszej dyrektywy i podjęły wszelkie środki niezbędne do ich wykonania. W projekcie ustawy znajduje się rozdział 8 („Przepis karne"), w którym zawarte są dwa przepisy karne. Penalizują one przetwarzanie danych osobowych niedopuszczalne lub bez uprawnienia (art. 54), jak również udaremnienie lub istotne utrudnienie przeprowadzanej kontroli przez kontrolującego z Urzędu Ochrony Danych Osobowych (art. 55). Odnosząc powyższe przepisy do obowiązków określonych

w projekcie ustawy, należy stwierdzić, że sankcje przewidziano za naruszenie zasad dopuszczalności przetwarzania danych osobowych (art. 13 i art. 14 projektu), jak również za kwalifikowane naruszenie obowiązków związanych z kontrolą (art. 5 ust. 1 pkt 7, art. 6 oraz art. 7 projektu ustawy), tj. tylko takie naruszenie, które prowadzi do udaremnienia lub istotnego utrudnienia kontroli. W przypadku innych przepisów projektowanej ustawy, a ściślej obowiązków w nich określonych, projektodawca nie przewiduje jakichkolwiek sankcji za ich naruszenie, czy to karnych, czy to administracyjnych (np. administracyjnych kar pieniężnych). Prowadzi to do sytuacji nie tylko niepełnego wykonania wymogu określonego w art. 57 dyrektywy 2016/680, ale także zagrożenia efektywności realizacji prawnych obowiązków przez ich adresatów, ponieważ nakładając na nich obowiązki, nie przewidziano żadnych sankcji za ich nieprzestrzeganie. Powyższa uwaga dotyczy w szczególności wskazanych w projekcie ustawy obowiązków zabezpieczenia danych osobowych, których niewykonanie nie jest zagrożone jakąkolwiek karą. Z punktu widzenia dyrektywy 2016/680 oznacza to również, że ze względu na niezmiernie zawężony zakres podlegających ochronie w przepisach karnych w zakresie prawnych zasad ochrony danych osobowych przepisy te nie mają charakteru skutecznego i odstraszającego, co jest wymagane w art. 57 zdanie drugie dyrektywy.

W projektowanej ustawie przewidziano bardzo zbliżone przepisy karne do tych zapisanych w ustawie o ochronie danych osobowych z 2018 r. (art. 107 i art. 108 tej ustawy). Jednak w tym wypadku przyjęcie w projektowanej ustawie takiego wzorca jest nieuzasadnione. Znajdujące się w ustawie z 2018 r. dwa przepisy karne mają jedynie charakter uzupełniający – w rozumieniu art. 84 RODO – w stosunku do podstawowego rodzaju sankcji za naruszenie przepisów o ochronie danych osobowych, jakim są przewidziane w RODO administracyjne kary pieniężne (zob. art. 83 RODO). Tymczasem dyrektywa 2016/680 w art. 57 nakazuje, aby całość systemu sankcji za naruszenie przepisów została przyjęta w prawie krajowym.

W zakresie prawnokarnej ochrony prawa do ochrony danych osobowych nastąpiło obniżenie poziomu ochrony względem ustawy o ochronie danych osobowych z 1997 r., biorąc pod uwagę zakres penalizowanych zachowań (działań lub zaniechań) stanowiących naruszenie przepisów o ochronie danych osobowych. W ustawie z 1997 r. znajdowało się aż 6 przepisów karnych. W szczególności ustawa przewidywała odpowiedzialność karną osób administrujących za naruszenie choćby nieumyślne obowiązku zabezpieczenia danych osobowych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem (art. 52 tej ustawy).

Podsumowanie

- Projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości ma na celu wykonanie prawa Unii

Europejskiej, tj. 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 uchylająca decyzję ramową Rady 2008/977/WSiSW. Jednak wskazane w opinii przepisy projektu budzą wątpliwości z punktu widzenia ich zgodności z dyrektywą oraz komplementarności z rozporządzeniem PE 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 (ogólne rozporządzenie o ochronie danych), jak również zapewnienia wysokiego poziomu ochrony danych osobowych. Dlatego też postulowane są w tym zakresie dalsze prace nad projektem.

- W dyrektywie 2016/680 nie występują podstawy prawne do wyłączenia stosowania określonych w dyrektywie przepisów o bezpieczeństwie danych osobowych w ramach całościowego wyłączenia spod mocy ustawy, o którym mowa art. 3 pkt 1 projektu ustawy.
- Dodatkowe okresy dostosowawcze na wdrożenie środków technicznych i organizacyjnych przewidziane w art. 103 ust. 1 i ust. 2 projektu ustawy nie są zgodne z zasadami określonymi w tym względzie w art. 63 dyrektywy 2016/680. Co więcej, przyjęcie ustawy w projektowanym kształcie sprawi, że między dniem wejścia w życie ustawy a dniem, w którym minie rok od wejścia w życie ustawy, podmioty zobowiązane mogą w zgodzie z ustawą nie stosować żadnej z podstawowych zasad bezpieczeństwa określonych w ustawie, co powoduje ryzyko dla faktycznego bezpieczeństwa danych.
- W projekcie nastąpiło rozproszenie regulacji w zakresie bezpieczeństwa danych osobowych w wielu aktach normatywnych, co nie sprzyja tworzeniu i stosowaniu uniwersalnych zasad bezpieczeństwa w podmiotach objętych mocą dyrektywy 2016/680.
- Projekt ustawy nie przewiduje podstawowego obowiązku administratora przy powierzaniu innym podmiotom przetwarzania danych osobowych, który został określony w art. 22 ust. 1 dyrektywy 2016/680, tj. obowiązku wyboru podmiotu świadczącego usługi gwarantującego wdrożenie odpowiednich środków technicznych i organizacyjnych zabezpieczających dane osobowe.
- W projekcie ustawy nie przewidziano jakichkolwiek sankcji za naruszenia obowiązków w zakresie bezpieczeństwa danych osobowych, co może zostać uznane za niewykonanie wymogu określonego w art. 57 dyrektywy 2016/680.