PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 17-06-2024

DOL.401.158.2024

Pan

Zastępca Szefa Kancelarii Sejmu RP

Szanowny Panie Ministrze,

w odpowiedzi na pismo z dnia 22 kwietnia 2024 r. znak: SPS-WP.020.119.5.2024, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] (dalej „rozporządzenie 2016/679") oraz art. 51 ustawy o ochronie danych osobowych[2], uprzejmie informuję, że Prezes Urzędu Ochrony Danych Osobowych (organ nadzorczy) zgłasza następujące uwagi do **poselskiego projektu ustawy o ochronie ludności oraz o stanie klęski żywiołowej (przedstawiciel wnioskodawców: poseł Paweł Szefernaker)** – dalej jako: „projekt ustawy".

Organ nadzorczy nie kwestionuje celu regulacji tworzonej na potrzeby stosownego reagowania w przypadkach zdarzeń losowych o trudnych do przewidzenia skutkach. Regulacja tworzona dla ochrony ludności w celu zapobiegania skutkom klęsk żywiołowych wymaga jednak zapewnienia stosowania w jej treści również przepisów unijnego rozporządzenia 2016/679 w celu zagwarantowania prawidłowego stosowania zasad dotyczących przetwarzania danych osobowych.

W omawianym przypadku, ze względu na projektowane nowe rozwiązania z udziałem nowych technologii – na szeroką skalę przetwarzania w wyjątkowych warunkach – wprowadzanym normom prawnym z zakresu przetwarzania danych osobowych powinien towarzyszyć **tzw. test prywatności – ocena skutków dla ochrony danych osobowych (art. 35 rozporządzenia 2016/679[3]), w tym**

---

[1] Rozporządzenie 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 4.5.2016, str. 1 ze zm.).

[2] Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

[3] Zgodnie z art. 35 ust. 1 rozporządzenia 2016/679 jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym

Urząd Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

tel. 22 531-03-88
fax 22 531-03-99

www.uodo.gov.pl

uwzględnienie ochrony danych w fazie projektowania oraz **domyślna ochrona danych (art. 25 ust. 1[4])**.

Należy podkreślić, że kształtowanie nowych procesów przetwarzania danych, poprzedzone musi być wykonaniem testu prywatności przeprowadzonym w związku z projektowaniem przedmiotowych regulacji. Jeżeli dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, projektodawca powinien uwzględnić przy określaniu sposobów przetwarzania ochronę danych w fazie projektowania. Celem takiego testu jest uwzględnienie oceny skutków przewidywanych rozwiązań prawnych dla ochrony danych, w tym przyjęcie przepisów szczegółowych zawierających rozwiązania zapewniające wyczerpującą, przejrzystą, prawidłową, właściwie wpisaną w system prawny regulację zapewniającą stosowanie przepisów o ochronie danych osobowych. Tymczasem z treści projektowanych przepisów i uzasadnienia projektu nie wynika, aby taka ocena została przeprowadzona przez projektodawcę. Test taki jest w tym przypadku zasadny z uwagi na projektowane modele przetwarzania danych, nowe powstające z tego tytułu zagrożenia o szczególnym charakterze w przypadku wystąpienia zdarzeń opisanych w ustawie, określenie nowych kategorii osób, objęcie zakresem regulacji szczególnych kategorii danych, ilość danych podlegających przetwarzaniu, zasadność przetwarzania ich za pośrednictwem nowych technologii. Okoliczności te ze względu na ich charakter, zakres, kontekst projektowanych przepisów i cele z dużym prawdopodobieństwem mogą powodować ryzyko naruszenia praw lub wolności osób fizycznych.

Przeprowadzenie takiej analizy powinno prowadzić do wykazania niezbędności przetwarzania wskazanych w przepisach danych osobowych w określony sposób, we wskazanym konkretnie celu (celach) i zakresie oraz oceny ryzyka projektowanych (przyjmowanych) rozwiązań w zakresie przetwarzania danych osobowych, a w konsekwencji wpływu na prywatność osób, których dane dotyczą – co pozwoli stworzyć normy bardziej przejrzyste od proponowanych i lepiej dostosowane do zasad przetwarzania danych osobowych. Poprawnie przeprowadzona ocena skutków dla ochrony danych powinna wskazywać związek pomiędzy operacjami wykonywanymi na danych osobowych z konkretnym celem ich przetwarzania, a wszelkie kluczowe decyzje związane z przetwarzaniem danych osobowych przez organy władzy publicznej powinny być określone w przepisach rangi ustawy. Rozwiązaniu polegającemu na przetwarzaniu danych osobowych przez szeroki krąg podmiotów wobec zamiaru wprowadzenia systemowych rozwiązań na wypadek zaistnienia klęsk żywiołowych

---

prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

[4] Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

powinien w opinii organu nadzorczego towarzyszyć test prywatności, przeprowadzony z uwzględnieniem **art. 35 ust. 1** rozporządzenia 2016/679 oraz ze szczególną analizą wskazanych w niniejszej opinii norm konstytucyjnych. Należy wziąć pod uwagę, że ochrona ludności stanowiąca podstawowy cel projektowanych przepisów na wypadek wystąpienia klęski żywiołowej jest pojęciem szerokim i powinna w tych okolicznościach być kształtowana także z uwzględnieniem określonych reguł unijnego prawa o ochronie danych osobowych.

Zakres i zasady przetwarzania danych osobowych

Wobec rodzaju i charakteru zdarzeń, których skutkom projekt ustawy ma zapobiegać, potrzeba stworzenia rozwiązań umożliwiających podjęcie szybkich działań jest w pełni uzasadniona. Projektowane przepisy nie powinny jednak tworzyć konstrukcji, które nie uwzględniają prawidłowości i bezpieczeństwa przetwarzanych danych osobowych, zgodnie z wymogami zawartymi w rozporządzeniu 2016/679. W myśl **art. 20** projektu ustawy, ministrowie kierujący działami administracji rządowej tworzą punkty kontaktowe realizujące zadania w obszarze ochrony ludności lub centra zarządzania kryzysowego (podobne zespoły o charakterze lokalnym mogą również tworzyć wojewodowie i starostowie). Z brzmienia tych przepisów nie wynika jednak, czy jednostki zarządzania kryzysowego będą przetwarzać dane osobowe – a jeśli tak – jakie to będą dane w założeniach projektodawcy. Nie wyjaśniono czy w toku tych działań przetwarzane mogą być tzw. dane wrażliwe (szczególne) określone w art. 9 rozporządzenia 2016/679 (podlegają one szczególnemu reżimowi przetwarzania) i jakie są planowane unormowania dotyczące przepływu takich informacji pomiędzy organami wchodzącymi w skład Rządowego Centrum Bezpieczeństwa. W przypadku przetwarzania szczególnej kategorii danych osobowych na wielką skalę przez szereg podmiotów powstaje także wątpliwość czy art. 20 projektu ustawy odpowiednio zabezpiecza zapewnienie przestrzegania zasad przetwarzania danych osobowych przez administratorów. Wątpliwości organu nadzorczego budzi również brzmienie **art. 23** projektu ustawy, zgodnie z którym „organy ochrony ludności mają prawo żądania udzielenia informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w ustawie, a ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, starostowie, wójtowie (burmistrzowie, prezydenci miast) przekazują niezwłocznie ministrowi właściwemu do spraw wewnętrznych informacje i wyjaśnienia niezbędne do realizacji zadań określonych w art. 9”. Proponowane brzmienie tego przepisu ma charakter bardzo ogólny, w żaden sposób nie określa zakresu informacji, którego może dotyczyć. Powstaje więc uzasadniona wątpliwość co do wystarczających gwarancji dla ochrony danych osobowych, w tym danych szczególnych kategorii, z uwagi na blankietowość przepisu. Odsyła on bowiem bardzo ogólnie do zadań określonych w ustawie, brak jest jednak określenia w ramach jakich zadań przetwarzane będą jakie dane osobowe (jakie ich kategorie).

Projektowane przepisy nie regulują też sposobu w jaki będą one przetwarzane, nie jest więc jasne czy będzie się to odbywać w formie żądania udzielenia informacji na wniosek czy też bez wniosku. Nie określono też podstawowych wymogów dotyczących

formy przekazywania tych informacji (ustnie/pisemnie/w postaci elektronicznej). Brak tych regulacji, szczególnie w czasie wystąpienia klęski żywiołowej, może skutkować poważnym ryzykiem naruszenia zasad przetwarzania danych osobowych, gdyż projektowane przepisy nie tworzą podstawowych ram i zasad w omawianym zakresie. W sytuacji takiej podmioty danych pozbawione są gwarancji przestrzegania ich praw.

Z brzmienia **art. 24** projektu ustawy nie wynika również czy zasoby ochrony ludności tworzone przez organy ochrony ludności mogą obejmować również dane osobowe i czy w takim razie ich przekazywanie może mieć miejsce poprzez zawierane porozumienia z innymi podmiotami ochrony ludności.

Zgodnie z **art. 36 ust. 1-3** projektu ustawy Prezes Rady Ministrów, ministrowie oraz wojewodowie mogą wydawać stosowne polecenia obowiązujące określone w nich podmioty. Nie jest jednak jasne czy polecenia te mogą odnosić się do kształtowania procesów przetwarzania danych osobowych. Odniesienie się przez projektodawcę do tej kwestii pozwoli na dokonanie oceny przyjętej regulacji w zakresie jej zgodności z zasadą legalizmu (art. 5 ust. 1 lit a rozporządzenia 2016/679), a także pozwoli wykazać proporcjonalność wprowadzanych ograniczeń w myśl **art. 51 Konstytucji RP**[5], gdyż zakres poleceń wydawanych w sferze publicznej powinien wynikać z ustawy, jeśli ma się odnosić do ograniczeń praw obywatelskich (zob. także art. 31 ust. 3 Konstytucji RP).

Podobne wątpliwości organu nadzorczego budzi również brzmienie **art. 55** projektu ustawy. W tym przypadku również nie jest jasne, czy polecenia te mają dotyczyć danych osobowych oraz czy mocą takich poleceń będą zmieniane cele przetwarzania danych u pierwotnych administratorów, w tym działających na podstawie obowiązujących przepisów. Nie jest wiadome również czy na podstawie takiego polecenia można zmieniać cel prowadzenia rejestru publicznego, łączyć dane z różnych baz danych, itp. Konstrukcja przepisów projektu ustawy wskazuje, że w przypadku braku realizacji polecenia zadanie przejmuje inny podmiot (który będzie pełnił rolę administratora) – wyjaśnienia ze strony projektodawcy wymaga więc, czy będzie to oznaczać, że ten nowy administrator będzie miał dostęp do wszelkich baz, rejestrów i danych prowadzonych przez organy samorządu terytorialnego. Projektodawca winien dokonać analizy czy w takiej sytuacji projektowane przepisy mają charakter kompleksowy i czy nie skutkują koniecznością dostosowania innych przepisów krajowych regulujących te kwestie, w szczególności przepisów kształtujących zakres przedmiotowo-podmiotowy prowadzenia rejestrów publicznych.

Obowiązek świadczeń osobistych i rzeczowych na rzecz ochrony ludności (ograniczenia wolności i praw człowieka i obywatela)

[5] Zgodnie z art. 51 Konstytucji RP: 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Możliwość wprowadzenia obowiązku świadczeń osobistych i rzeczowych na rzecz ochrony ludności przewiduje **art. 49 ust. 1 pkt 21** projektu ustawy. Jednocześnie zgodnie z **art. 50 ust. 4** projektu ustawy „Rada Ministrów może określić, w drodze rozporządzenia, sposób wykonywania świadczeń osobistych lub rzeczowych na rzecz ochrony ludności, mając na uwadze zapewnienie prawidłowego ich wykonania". Konstrukcja tego przepisu wskazuje, że akt wykonawczy będzie również stanowił podstawę przetwarzania danych osobowych w toku wykonywania świadczeń osobistych i rzeczowych. Tymczasem, zgodnie z **art. 7 Konstytucji RP**[6]**,** organy władzy publicznej działają na podstawie i w granicach prawa – zasada legalizmu odnosi się także do praw i obowiązków związanych z przetwarzaniem danych osobowych. W art. 6 ust. 1 lit. c rozporządzenia 2016/679 wskazano wymóg tworzenia regulacji, z których będzie wynikał ściśle określony obowiązek, dla którego realizacji niezbędne jest przetwarzanie danych osobowych. Podstawa prawna przetwarzania danych osobowych powinna przewidywać elementy określone w art. 6 ust. 3 rozporządzenia 2016/679[7]. W omawianym przypadku szczególne znaczenie ma określenie ww. „operacji i procedur przetwarzania" w kontekście wyrażonych w art. 5 ust. 1 lit. a oraz art. 5 ust. 2 rozporządzenia 2016/679[8] zasad zgodności z prawem, rzetelności i przejrzystości oraz rozliczalności. Określenie podstawy prawnej dla przetwarzania danych osobowych przez podmioty publiczne wymaga sformułowania obowiązku, a zatem wyartykułowania niezbędności przetwarzania danych osobowych w zakresie celów, w których są przetwarzane (art. 5 ust. 1 lit. c rozporządzenia 2016/679)[9]. Wykonawcy norm o charakterze publiczno-prawnym, którzy w rozumieniu przepisów rozporządzenia 2016/679 dla wykonywania projektowanych regulacji pełnić będą rolę administratorów, nie powinni mieć pozostawionej tak szerokiej swobody interpretacyjnej w sferze realizacji obowiązków dotyczących przetwarzania danych osobowych, a także być pozostawieni w sytuacji niepewności prawnej w zakresie wydania aktu wykonawczego. Dotyczy to również szczególnej kategorii danych osobowych określonych w **art. 9**

---

[6] Art. 7 [Zasada praworządności] Organy władzy publicznej działają na podstawie i w granicach prawa.

[7] Zgodnie z art. 6 ust. 3 rozporządzenia 2016/679:
Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

[8] Zgodnie z art. 5 ust. 1 lit. a rozporządzenia 2016/679 dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (,,zgodność z prawem, rzetelność i przejrzystość"). Zgodnie z art. 5 ust. 2 rozporządzenia 2016/679
administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie (,,rozliczalność").

[9] Zgodnie z art. 5 ust. 1 lit. c rozporządzenia 2016/679 dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

rozporządzenia 2016/679, podlegających szczególnemu reżimowi przetwarzania. Zgodnie z **art. 49 ust. 1 pkt 7** projektu ustawy ograniczenia wolności i praw obywatelskich mogą również polegać na obowiązku poddania się badaniom lekarskim, leczeniu oraz stosowaniu innych środków profilaktycznych i zabiegów niezbędnych dla zwalczania chorób zakaźnych oraz skutków skażeń chemicznych i promieniotwórczych. Uzasadnienie wprowadzenia ww. obowiązku w określonych okolicznościach nie budzi większych wątpliwości organu nadzorczego, projektodawca winien jednak wziąć pod uwagę szeroki zakres przetwarzanych danych różnych kategorii w procesie tworzenia systemowych rozwiązań technicznych i informatycznych, które zapewnią ich bezpieczeństwo celem poszanowania zasady integralności i poufności wynikającej z art. 5 ust. 1 lit f rozporządzenia 2016/679. Pamiętać ponadto należy, że zgodnie z art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw (w tym prawa do ochrony danych osobowych uregulowanego w jej art. 51) mogą być ustanawiane **tylko w ustawie** i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób.

Co więcej, projektodawca w **art. 51** projektowanej ustawy umożliwia wójtom (burmistrzom, prezydentom miast), starostom, a także wojewodom, „niezbędne ograniczenia wolności i praw człowieka i obywatela, o których mowa w art. 40 oraz obowiązki świadczeń osobistych i rzeczowych, o których mowa w art. 50, w granicach dopuszczonych w rozporządzeniu Rady Ministrów o wprowadzeniu stanu klęski żywiołowej wprowadzać (…) w drodze zarządzenia albo decyzji". Niezależnie od oceny zgodności takich rozwiązań z perspektywy konstytucyjnego testu proporcjonalności i legalizmu, wprowadzanie tych ograniczeń na mocy zarządzenia czy decyzji nie może prowadzić do obniżenia w sposób nieproporcjonalny praw i wolności osób, których dane dotyczą. Kształtowanie mocą takich aktów procesów przetwarzania danych osobowych powinno uwzględniać art. 23 rozporządzenia 2026/679 i wytyczne EROD dotyczące jego stosowania[10].

Z podobnych względów wątpliwości organu nadzorczego budzą również rozwiązania zawarte w **art. 51 ust. 4 pkt 2** projektu ustawy, który przewiduje, że decyzje, o których mowa w art. 51 ust. 1 projektu „w uzasadnionych przypadkach mogą być wydawane i przekazywane ze skutkiem wiążącym także ustnie, pisemnie w formie adnotacji, telefonicznie, za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną lub za pomocą innych środków łączności, a treść oraz istotne motywy takiego załatwienia sprawy utrwala się w formie pisemnej". Przyjęcie takich rozwiązań powinno być poprzedzone wykonaniem testu proporcjonalności i oceną ryzyk dla przetwarzania danych osobowych, tak aby nie dochodziło nawet w tak szczególnym czasie do wyłączenia praw podmiotów danych i naruszenia zasad ochrony danych osobowych (np. ryzyko przekazywania ustnego danych osobowych, w tym szczególnych kategorii osobom nieuprawnionym).

---

[10] Wytyczne 10/2020 Europejskiej Rady Ochrony Danych w sprawie ograniczeń na podstawie art. 23 RODO, https://www.edpb.europa.eu/system/files/2023-07/edpb_guidelines_202010_art23_adopted_afterpublicconsultation_pl.pdf (dostęp: 14.06.2024 r.).

Powstają także wątpliwości co do zapewnienia zgodności projektowanych rozwiązań z zasadą ograniczenia przechowywania (art. 5 ust. 1 lit. e rozporządzenia 2016/679). O ile przy realizacji zadań wskazanych w projekcie ustawy powstawać będą nowe bazy i rejestry, należy ocenić zakres danych w nich przechowywanych i okres tego przechowywania tak, aby jednocześnie odbyło się to bez uszczerbku spełnienia zakładanych celów ustawy.

Kolejna uwaga dotyczy projektowanego **art. 51 ust. 2 i 3,** zgodnie z którym ogłoszenie rozporządzeń porządkowych i zarządzeń następuje w formie rozplakatowania „obwieszczeń" (niespójność językowa) w miejscach publicznych lub w inny miejscowo przyjęty sposób, a także przez ogłoszenie w lokalnej prasie, które zawiera „określenie obowiązanych podmiotów". Konstrukcja tego przepisu nie jest jednoznaczna pod względem określenia czy w obwieszczeniach znajdą się także dane osobowe, a jeżeli tak to jakie (jakich to dotyczyć będzie obowiązanych podmiotów). Wyjaśnienie tej kwestii umożliwi dokonanie oceny stopnia realizacji zasad ochrony danych osobowych (w tym zasady proporcjonalności, integralności i poufności, jak również ograniczenia czasowego)[11].

Pomocniczo należy wskazać sposób rozwiązania zagadnień związanych z wykonywaniem obowiązków osobistych i rzeczowych w art. 618-636 ustawy z dnia 11 marca 2022 r. o obronie ojczyzny (Dz. U. z 2024 r. poz. 248) wraz z aktami wykonawczymi wydanymi na ich podstawie.

Szczególne rozwiązania w związku z wystąpieniem klęski żywiołowej

Wątpliwa jest zasadność, celowość i adekwatność żądania wskazywania miejsca zamieszkania pracownika w wykazie pracowników dołączanym przez pracodawcę do wniosku o udzielenie pożyczki z Funduszu Gwarantowanych Świadczeń Pracowniczych w przypadku braku środków na wypłatę pracownikom wynagrodzenia w wyniku klęski żywiołowej (**art. 82 ust. 14 projektowanej ustawy**). Projektodawca nie wykazał niezbędności pozyskiwania danych osobowych na etapie analizy zasadności przyznania pomocy finansowej pracodawcy. Na powtórną analizę zasługuje także wymóg złożenia podpisu przez pracownika na wniosku pracodawcy, który zaprzestaje działalności w wyniku klęski żywiołowej – w ocenie organu nadzorczego wymóg taki może być nieadekwatny do zakładanych stanów faktycznych.

Podobna uwaga dotyczy **art. 88 ust. 2 pkt 1 lit. b oraz art. 103 ust. 3 pkt 4 lit. c** projektu ustawy – data urodzenia ma charakter wtórny i zbędny w przypadku przetwarzania numeru PESEL (byłoby to zasadne wyłącznie w przypadku braku nadania tego numeru), a jednocześnie w polskim systemie prawnym brak jest obowiązku posiadania telefonu; przetwarzanie danej określonej jako „telefon kontaktowy" nie może więc mieć charakteru obligatoryjnego. Jednocześnie katalog danych zawarty w art. 88 ust. 2 pkt 1 projektu ustawy poprzez użycie wyrażenia „w tym"

[11] Zgodnie z art. 5 ust. 1 lit. f rozporządzenia 2016/679 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.

jest otwarty, a przez to kształtuje bliżej nieokreślony dodatkowy zakres pozyskiwanych danych osobowych, co może prowadzić do naruszenia zasady proporcjonalności. W każdym przypadku katalog przetwarzanych danych osobowych powinien mieć charakter zamknięty i jednoznacznie określać dane niezbędne do celów przetwarzania, aby uniknąć wątpliwości interpretacyjnych zarówno adresatów, jak i wykonawców norm. Projektodawca powinien wskazać co najmniej minimalne kryteria wymagane od wykonawców norm w kontekście art. 24[12], 32[13] oraz 35[14] rozporządzenia 2016/679

---

[12] Zgodnie z art. 24 rozporządzenia 2016/679: 1.Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. 2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych. 3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

[13] Zgodnie z art. 32 rozporządzenia 2016/679: 1.Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: a) pseudonimizację i szyfrowanie danych osobowych; b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. 2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42. 4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

[14] Zgodnie z art. 35 rozporządzenia 2016/679: 1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. 3.Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku: a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie. 7.Ocena zawiera co najmniej:
a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób,

również z uwzględnieniem szczególnego reżimu ochrony przetwarzania krajowego numeru identyfikacyjnego, wynikającego z art. 87[15] rozporządzenia 2016/679 (jak już to wyżej wyjaśniono, dane te mogą być szczególnie zagrożone w przypadku wystąpienia klęski żywiołowej). Wątpliwości organu nadzorczego wzbudza również konieczność dołączania oświadczenia o „wyrażeniu zgody na weryfikację danych zawartych we wniosku" do wniosku poszkodowanego o pomoc finansową (**art. 88 ust. 2 pkt 9a oraz art. 89 ust. 2 pkt 8a** projektowanej ustawy). Należy wskazać, że każdorazowo składana zgoda na przetwarzanie danych osobowych musi być dobrowolna i niewymuszona. Wyrażający zgodę może ją ponadto w każdym czasie odwołać. Jeżeli natomiast przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego (art. 6 ust. 3 rozporządzenia 2016/679).

Zgodnie z **art. 103 ust. 5** projektu ustawy „dane do rejestru przekazywane są z: rejestru PESEL, Centralnej Ewidencji Kierowców i ewidencji wojskowej". Przepis ten – jest blankietowy - nie określa bowiem: 1) trybu przekazywania opisanych danych osobowych, 2) ról podmiotów w procesach przetwarzania danych osobowych, 3) wymogu złożenia wniosku przez ministra właściwego do spraw wewnętrznych, 4) środków technicznych, za pomocą których przekazuje się te dane z uwzględnieniem ich bezpieczeństwa, zasad przeglądu i aktualizacji danych oraz ich retencji. Regulacja ta nie spełnia wobec tego wymogów określonych w art. 5 ust. 1 lit. a, lit. d[16], lit. e[17] i lit. f oraz motywie 31[18] rozporządzenia 2016/679. Stanowisko organu nadzorczego znajduje

---

których sprawa dotyczy. 10. Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

[15] Zgodnie z art. 87 rozporządzenia 2016/679 państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie.

[16] Zgodnie z art. 5 ust. 1 lit. d rozporządzenia 2016/679 dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (,,prawidłowość").

[17] Zgodnie z art. 5 ust. 1 lit. e rozporządzenia 2016/679 dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą (,,ograniczenie przechowywania").

[18] Zgodnie z motywem 31 rozporządzenia 2016/679 organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), nie powinny być traktowane jako

potwierdzenie w wyroku TSUE (trzecia izba) z dnia 1 października 2015 r. (Smaranda Bara i in. przeciwko Președintele Casei Naționale de Asigurări de Sănătate i in. – w szczególności od pkt 28 na str. 9)[19]. Zaproponowany sposób regulacji skutkuje zmianą pierwotnych celów przetwarzania danych w określonych rejestrach, a to wymaga wprowadzenia określonych gwarancji dla podmiotów danych i zapewnienia poszanowania realizacji zasady rozliczalności przez administratorów prowadzących rejestry i udostępniających z nich dane osobowe.

Tryby prac zespołów, sztabów i komisji

Brak jest w projektowanych przepisach kompleksowych rozwiązań dotyczących porozumiewania się na odległość w formach zapewniających bezpieczeństwo przetwarzania danych osobowych, weryfikację uczestników spotkań i obrad oraz zabezpieczenie przed cyberzagrożeniami. W zapobieganie cyberzagrożeniom wpisany powinien być tak istotny aspekt jak przetwarzanie, w tym ochrona danych osobowych z zapewnieniem stosowania obowiązujących przepisów z tej dziedziny. W opinii organu nadzorczego jest to szczególnie istotne wobec perspektywy konieczności podjęcia szeregu działań o pilnym charakterze zespołowym (sztaby kryzysowe) w okolicznościach ograniczających sprawne przemieszczanie się, w tym w szczególności w zakresie osób dodatkowo zapraszanych na stosowne posiedzenia/obrady, jak przykładowo w **art. 8 i 19** projektu ustawy, które dotyczą określenia zasad organizacji prac Rządowego Zespołu Zarządzania Kryzysowego oraz zespołów zarządzania kryzysowego. Określenie „wybór trybu pracy" przez dany zespół, bez określenia jakie projekt ustawy tryby pracy przewiduje – oraz na jakich warunkach, przy użyciu jakich środków technicznych i organizacyjnych – jest zbyt lakoniczne, szczególnie wobec szeregu cyberzagrożeń towarzyszących porozumiewaniu się na odległość, jak również przy udziale zaproszonych osób trzecich. Nieuprawnione ujawnienie przebiegu takich obrad, ich ustaleń skutkować może poważnymi zagrożeniami nie tylko w sferze ochrony prywatności i danych osobowych, ale także w aktualnych okolicznościach geopolitycznych - zagrażać może infrastrukturze i bezpieczeństwu państwa w sytuacjach krytycznych (projekt ustawy nie reguluje również kwestii dotyczących ewentualnej rejestracji prac powoływanych zespołów). Uregulowanie tych kwestii, z uwzględnieniem zasad dotyczących przetwarzania danych osobowych wpisuje się w istotny cel, jakim jest podwyższenie zabezpieczeń zapobiegających cyberzagrożeniom[20].

---

odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

[19] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A62014CJ0201 (dostęp 16.05.2024 r).

[20] Pomocniczo należy wskazać w tym miejscu na wyrok Naczelnego Sądu Administracyjnego z 28 lutego 2024 r. w sprawie o sygn. akt II OSK 3839/21, który oddalił skargę kasacyjną burmistrza i tym samym podtrzymał decyzję Prezesa UODO o nałożeniu kary za naruszenie przepisów rozporządzenia 2016/679 wynikającą z dokonania rejestracji i publikacji obrad sesji rady miasta na kanale nienależącym do

Określanie infrastruktury krytycznej oraz zapewnianie ciągłości jej funkcjonowania

Zgodnie z **art. 124 ust. 4** projektu ustawy „w należycie uzasadnionych przypadkach podmiot krytyczny może składać wnioski o sprawdzenie przeszłości osób, które: a) pełnią newralgiczne role w podmiocie krytycznym lub na jego rzecz, w szczególności w odniesieniu do odporności podmiotu krytycznego; b) są upoważnione do posiadania bezpośredniego lub zdalnego dostępu do budynków i terenów podmiotu krytycznego, jego informacji lub systemów kontroli, w tym w związku z bezpieczeństwem podmiotu krytycznego; c) są brane pod uwagę przy rekrutacji na stanowiska objęte kryteriami, określonymi w lit. a) lub b)". W opinii organu nadzorczego użyte przez projektodawcę pojęcie „sprawdzania przeszłości" jest nieprecyzyjne, niejednoznaczne i budzi poważne wątpliwości dotyczące potencjalnego zakresu danych osobowych podlegających przetwarzaniu. Nie jest również jasne z jakich źródeł (baz, rejestrów) prowadzonych przez jakich administratorów podmiot uprawniony do weryfikacji przeszłości danej osoby może korzystać. Nie wskazano też zasad dostępu do tych informacji, tj. na jakich zasadach i w jakim trybie dostęp ten jest możliwy. Wyjaśnienia wymaga również, czy czynność ta może dotyczyć przetwarzania danych osób trzecich (np. członków rodziny) oraz czy i jak projektodawca planuje zagwarantować spełnienie obowiązku informacyjnego względem wszystkich osób podlegających weryfikacji. W opinii organu nadzorczego przepis ten wymaga uzupełnienia również o jednoznaczne ramy czasowe takiej weryfikacji wstecz oraz o wskazanie trybu dokonania tej czynności (to z przepisów ustawy powinno wynikać, czy podejmowane są one np. w trybie niejawnym).

Podsumowanie

Kształt przedstawionego do opinii projektu ustawy nie znajduje zgodnie z powyższą argumentacją pełnego oparcia w wymogach przewidzianych przepisami rozporządzenia 2016/679, jak również budzi wątpliwości co do spełnienia standardów konstytucyjnych. Projektodawca tworzy szereg niejasnych i nieprecyzyjnych konstrukcji bez wskazania jednoznacznych trybów procedowania, zamkniętych katalogów danych adekwatnych do ratio legis projektu, posługuje się niespójnym i niezdefiniowanym nazewnictwem, a także odsyła do treści aktów wykonawczych (w tym nieobligatoryjnych) bez zapewnienia podstawowych regulacji ustawowych. Kwestie te mają szczególne znaczenie wobec objęcia zakresem przetwarzania przez przedstawiony projekt ustawy danych osobowych znacznej ilości osób o zróżnicowanym charakterze i rodzajach, w tym danych z art. 9 i 10 rozporządzenia 2016/679. Nawet w tak szczególnym okresie, jak opisany w projekcie należy pamiętać o zapewnieniu poszanowania standardów ochrony danych osobowych. Zwróciła na to

---

administratora. NSA oddalając skargę podtrzymał argumenty podnoszone przez Prezesa UODO i zgodził się z wcześniejszym wyrokiem WSA w Warszawie o sygn. akt II SA/Wa 2826/19 z 26 sierpnia 2020 r.

uwagę Europejska Rada Ochrony Danych osobowych podczas pandemii Covid-19. W „oświadczeniu w sprawie przetwarzania danych osobowych w kontekście pandemii COVID-19” z dnia 19 marca 2020 r. przewodnicząca Europejskiej Rady Ochrony Danych Osobowych podkreśliła, że nawet w tej wyjątkowej sytuacji administrator oraz podmiot przetwarzający muszą zapewnić ochronę danych osobowych i w związku z tym należy wziąć pod uwagę szereg czynników gwarantujących zgodne z prawem przetwarzanie danych a podejmowane w tym kontekście środki muszą być zgodne z ogólnymi zasadami ochrony danych i nie mogą być nieodwracalne. Sytuacja nadzwyczajna jest warunkiem prawnym, który może uzasadniać ograniczenie wolności, ale pod warunkiem, że ograniczenia te są proporcjonalne i ograniczone do okresu nadzwyczajnego[21].

Uwagi organu nadzorczego – co należy podkreślić – mają charakter wskazówek eksperckich, a za ostateczną zgodność projektowanych przepisów z Konstytucją RP oraz rozporządzeniem 2016/679 odpowiada projektodawca. Liczę, że niniejsze uwagi będą pomocne w realizacji tego zadania.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

[21] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_pl_1.pdf (dostęp: 14.06.2024 r.).