Warszawa, 19-03-2025

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

DOL.401.387.2024.WL.EKR

Pani
Katarzyna Bis-Płaza
Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji

elektroniczna skrzynka podawcza
ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z przekazanym do wiadomości organu nadzorczego pismem z 12 marca 2025 r. (znak: DPiS.WWKS.002.44.1.2025), w celu rozpatrzenia przez osoby uczestniczące w posiedzeniach Komitetu Rady Ministrów do spraw Cyfryzacji **projektu ustawy o Krajowym Rejestrze Oznakowanych Psów i Kotów**, dalej: projekt ustawy, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], Prezes UODO jako organ nadzorczy przedstawia poniżej następujące uwagi.

Prezes UODO w toku prac legislacyjnych nad projektem ustawy, na etapie opiniowania przedstawił projektodawcy uwagi pismem z 31 października 2024 r. (sygn. DOL.401.387.2024.MP). Pozytywnie należy ocenić uwzględnienie szeregu uwag wniesionych przez organ właściwy w sprawie ochrony danych osobowych, w tym jedną z najistotniejszą z podnoszonych kwestii, tj. dostępu do danych osobowych gromadzonych w rejestrze. Zrezygnowano bowiem z rozwiązania, które daje możliwość dostępu do danych gromadzonych w Rejestrze Oznakowanych Psów

[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).

i Kotów, dalej: KROPiK, każdemu kto posiada numer transpondera, tym samym zawężono krąg podmiotów mających dostęp do danych gromadzonych w rejestrze do enumeratywnie wymienionych w art. 15 projektu ustawy. Uzupełniony został również art. 2 ust. 5 projektu ustawy, który obecnie precyzuje cel w jakim gromadzone są dane osobowe w KROPiK. Doprecyzowany został także art. 6 projektu ustawy, który w obecnym brzmieniu jednoznacznie wskazuje jaki transponder uznaje się za właściwy.

Niemniej jednak **postulaty organu nadzorczego, które nie zostały do tej pory uwzględnione, pozostają nadal aktualne**. Przede wszystkim należy zwrócić uwagę, że dostęp do danych w KROPiK powinien ograniczony być jedynie do celu wykonywania zadań ściśle powiązanych z celami projektowanej ustawy i jedynie w zakresie danych w istocie niezbędnych do realizacji czynności związanych z tymi celami. Cele te powinny zostać jasno, konkretnie i zawężająco określone lub enumeratywnie wymienione w zamkniętym katalogu. Dlatego użyte w art. 15 ust. 1 projektu ustawy blankietowe pojęcie „przeszukiwania" rejestru, czy też sformułowanie „w celu niezbędnym do realizacji ich ustawowych zadań" powinny zostać doprecyzowane, celem wyeliminowania ewentualnych ryzyk związanych z nieuprawnionym pozyskiwaniem i dalszym przetwarzaniem danych. Kwestia ta była podnoszona i została szerzej opisana w dotychczasowej opinii organu nadzorczego.

Rejestracja psów i kotów w KROPiK wiąże się z przetwarzaniem danych osobowych ich posiadaczy za pomocą **nowo tworzonego systemu teleinformatycznego**, wielkiej bazy danych, w której dane osobowe są przetwarzane nie tylko na bardzo dużą skalę, ale również w szerokim zakresie. Determinuje to wypracowanie optymalnych rozwiązań informatycznych już we wstępnej fazie ich tworzenia. Z tych względów niezbędne jest przeprowadzenie testu prywatności, oceny skutków wprowadzanych rozwiązań i ryzyk związanych z przetwarzaniem danych osobowych. Powinien on obejmować rozwiązania zapewniające stosowanie rozporządzenia 2016/679, w tym określone w art. 5 rozporządzenia 2016/679 zasady

ochrony danych osobowych[3], w szczególności zgodności z prawem, rzetelności i przejrzystości, ograniczenia przechowywania, integralności i poufności oraz zasadę rozliczalności. Stosownej analizie powinny zatem zostać poddane: otoczenie prawne, zakres, cel pozyskiwania i dalszego przetwarzania danych w odniesieniu do funkcjonalności projektowanego systemu. Wiązać się to powinno z przeprowadzeniem kompleksowej oceny skutków dla ochrony danych

[3] Dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
d) 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");
e) 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");
f) 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 ("integralność i poufność").
2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

odpowiadającej wymogom art. 25 ust. 1 [4] i 2 [5] i art. 35 ust. 1 [6], 7 [7] rozporządzenia 2016/679, w toku której zostanie wykazana podstawa prawna dla przetwarzania danych osobowych w kontekście funkcjonowania systemu teleinformatycznego.

W „**Liście kontrolnej osiągania interoperacyjności przez system teleinformatyczny regulowany przez projekt dokumentu rządowego**” wskazane jest, że system będzie korzystał z danych referencyjnych przechowywanych w innym systemie teleinformatycznym – rejestrze PESEL. Należy zatem przypomnieć, że rejestry prowadzone są w konkretnych wskazanych w przepisach prawa celach, w których też przetwarzane są dane osobowe w nich zgromadzone. Pozyskiwanie przez organ publiczny danych z innych zbiorów danych powinno odbywać się z poszanowaniem zasad i gwarancji wynikających z rozporządzenia 2016/679, a integracja systemów nie może prowadzić do niedozwolonego łączenia rejestrów publicznych (zob. motyw 31 RODO[8]). Przepisy wdrażające tego rodzaju rozwiązania

---

[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”.

[5] „Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych”.

[6] „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”.

[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, których sprawa dotyczy”.

[8] „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 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”.

powinny szczegółowo określać procedurę, formę, zakres i tryb udostępniania danych osobowych.

Art. 10 ust. 1 pkt 2 projektu ustawy stanowi, że lekarz weterynarii dokonuje rejestracji psa lub kota w KROPiK przy użyciu „usługi sieciowej udostępnionej przez Agencję". Ze względu na architekturę tworzonego systemu istotne jest by projektowane przepisy były precyzyjne. Wyjaśnienia zatem wymaga o jaką usługę w tej normie chodzi oraz na jakich zasadach jest ona powiązana z system. W ww. przepisie mowa jest o zapewnieniu rozliczalności przez system teleinformatyczny. **Obowiązek zapewnienia rozliczalności spoczywa na administratorze i to jemu powinien być on przypisany wprost, jako podmiotowi praw i obowiązków**. System, jako narzędzie techniczno-organizacyjne, powinien oczywiście zapewnieniu rozliczalności sprzyjać, ale rolę tę powinien spełniać administrator (podmiot nie narzędzie).

Art. 10 ust. 2 projektu ustawy odnosi się do zasad rozporządzenia 2016/679, powołuje się na integralność czy zapewnienie bezpieczeństwa danych osobowych. Bez względu na treść ustawy, na administratorze spoczywał będzie obowiązek zapewnienia przestrzegania wszystkich zasad i unormowań rozporządzenia 2016/679. Rola administratora ma kluczowe znaczenie w stosowaniu przepisów rozporządzenia 2016/679, ponieważ to administrator jest adresatem szeregu obowiązków i praw wynikających z tego aktu prawnego. Odpowiada on m.in. za zgodność przetwarzania z zasadami określonymi tymi przepisami, w tym z art. 5 rozporządzenia 2016/679, za realizację praw osób, których dane dotyczą, wynikających z przepisów art. 13 i 14, 15–22 rozporządzenia 2016/679, a także jest obciążony pełną odpowiedzialnością za zgodne z prawem przetwarzanie danych, które prowadzi samodzielnie lub które prowadzone jest w jego imieniu.

Tworzenie regulacji krajowej niespójnej z rozporządzeniem 2016/679 nie sprzyja wykonawcom norm w przestrzeganiu obowiązujących i wprowadzanych przepisów. Odnosząc się zaś do bezpieczeństwa danych osobowych, warto już na poziomie ustawowym nakreślić kryteria zapewnienia bezpieczeństwa zgodne z wymaganiami rozporządzenia 2016/679.

Art. 12 projektu ustawy stanowi o przeprowadzaniu testów integracyjnych. Należy podkreślić, że przeprowadzanie testów integracyjnych nie może odbywać się za pomocą rzeczywistych danych osobowych, brak jest w tym zakresie niezbędności takich działań dla weryfikacji sprawności systemu.

Urząd Ochrony Danych Osobowych jednocześnie deklaruje swoje eksperckie wsparcie w zakresie propozycji tworzonych/nowelizowanych aktów prawnych i oceny ich zgodności z przepisami rozporządzenia 2016/679.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pan
Czesław Siekierski
Minister Rolnictwa i Rozwoju Wsi
Ministerstwo Rolnictwa i Rozwoju Wsi

elektroniczna skrytka podawcza
ePUAP: /5s4i53wlll/SkrytkaESP