PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 6.9.2024 r.

DOL.401.121.2024.WL.RB

Pani
Wioletta Zwara
Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji

ul. Królewska 27
00-060 Warszawa
ePUAP**:** /MAiC/SkrytkaESP

Szanowna Pani,

w odpowiedzi na pismo otrzymane 29 sierpnia br. (znak: DPiS.WWKS.002.122.1.2024) dotyczące **projektu ustawy o zmianie niektórych ustaw w celu deregulacji prawa gospodarczego i administracyjnego oraz doskonalenia zasad opracowywania prawa gospodarczego** (dalej: „projekt”), 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] uprzejmie informuję, że do przedstawionego projektu Prezes Urzędu Ochrony Danych Osobowych, jako organ nadzorczy, przedstawia następujące uwagi.

W **art. 29 zmiana 2** projektu zawarto propozycję dodania **art. 30a** do ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236 i 1222), który dotyczy sposobu ustalania umocowania pełnomocnika lub prokurenta na podstawie wpisów do Krajowego Rejestru Sądowego (dalej: KRS) lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej (dalej: CEiDG). Organ nadzorczy odnosił się już do tej kwestii w poprzednim piśmie skierowanym w tej sprawie do Ministerstwa Rozwoju i Technologii (sygn. DOL.401.121.2024.WL.RB). Na aprobatę

[1] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 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 dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 1781).

zasługuje ograniczenie oraz wskazanie wprost rejestrów dających możliwość do potwierdzania istnienia umocowania. Nadal jednak aktualne jest stanowisko co do tego, że przepisy wdrażające pozyskiwanie danych z innych rejestrów przez organy publiczne powinny szczegółowo określać procedurę, formę, zakres i tryb udostępniania danych osobowych. Jasna i zrozumiale określona powinna być procedura pozyskiwania i weryfikowania danych osobowych pełnomocnika zawartych w innych rejestrach. Tym bardziej, że zgodnie z proponowanym brzmieniem przepisu organ „z urzędu" potwierdza umocowanie pełnomocnika lub prokurenta w CEiDG albo KRS – niejasne jest więc czy również w przypadku okazania przez pełnomocnika lub prokurenta oryginału lub urzędowo poświadczonego odpisu pełnomocnictwa organ ma obowiązek każdorazowo potwierdzić istnienie umocowania w CEiDG albo KRS. Takie rozwiązanie powodowałoby wątpliwości co do celowości przedstawiania oryginału lub odpisu pełnomocnictwa oraz sprzeczne byłoby z zasadą minimalizacji danych z art. 5 ust. 1 lit. c rozporządzenia 2016/679[3]. Wyjaśnienia i dookreślenia wymaga sposób postępowania w sytuacjach, w których pełnomocnictwo udzielane jest w różnym zakresie w zależności od rodzaju sprawy – w jaki sposób w takich przypadkach weryfikowane będzie pełnomocnictwo oraz co do tego czy weryfikacja dotyczyć będzie tożsamości pełnomocnika czy faktu jego umocowania.

W **art. 29 zmiana 4 lit. b** projektu dodawany jest **art. 47 ust. 1a** do ustawy Prawo przedsiębiorców dotyczący udostępniania okresowego planu kontroli oraz okresowej analizy prawdopodobieństwa naruszenia prawa przez przedsiębiorcę w Biuletynie Informacji Publicznej (dalej: „BIP"). Organ nadzorczy podtrzymuje swoje stanowisko w tym zakresie przedstawione w poprzednim piśmie i zwraca uwagę, że ograniczenie udostępniania informacji ze względu na prywatność osoby fizycznej jest sformułowaniem zbyt ogólnym z punktu widzenia przepisów o ochronie danych osobowych. Prawodawca powinien w tym zakresie wprost wskazać na zakres udostępnianych danych osobowych, ich charakter, jak i okres retencji danych. Należałoby doprecyzować materię udostępniania informacji zawierających dane osobowe osoby fizycznej z uwzględnieniem zasad wynikających z rozporządzenia 2016/679, m.in. minimalizacji danych oraz ograniczenia celu[4] wraz z poszanowaniem reguł wynikających z art. 5 ust. 2[5] ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).

W **art. 29 zmiana 7 lit. b** projektu dodawany jest **art. 48 ust. 12** do ustawy Prawo przedsiębiorców, w którym ustanawiana jest „możliwość" udostępnienia

---

[3] Dane osobowe muszą być: c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych").

[4] Dane osobowe muszą być: 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").

[5] Prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

organowi kontroli, w czasie trwania kontroli, innych dokumentów i informacji związanych z zakresem przedmiotowym kontroli. Organ nadzorczy podtrzymuje swoje uwagi zawarte w tym zakresie w poprzednim piśmie. Z uwagi na konstytucyjną zasadę legalizmu (art. 7 Konstytucji RP) przepisy prawa – w materii związanej z przetwarzaniem danych osobowych - powinny kreować ściśle określone obowiązki organów państwowych, a nie jedynie ich „możliwości". Należy zwrócić uwagę, że żądanie innych dokumentów i informacji, a tym samym danych w nich zawartych, związanych z zakresem przedmiotowej kontroli musi wynikać z niezbędności ich przedstawienia i być zgodne z zasadą minimalizacji danych (art. 5 ust. 1 lit. b i c rozporządzenia 2016/679).

W **art. 32 zmiana 4** projektu proponowane jest dodanie **art. 508a** do ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 i 1720), który przewiduje możliwość przeprowadzenia rozpraw lub posiedzeń jawnych na odległość przy użyciu urządzeń technicznych. Należy zwrócić uwagę, że zapisanie obrazu i dźwięku z czynności procesowych odbywających się na sali rozpraw oznacza m.in. przetwarzanie danych osobowych. Z tego względu proces ten powinien odbywać się z poszanowaniem zasad wynikających z rozporządzenia 2016/679 (m.in. zasady minimalizacji danych oraz integralności i poufności[6]) i prawodawca w procesie tworzenia przepisów powinien w tym zakresie kierować się również kryterium bezpieczeństwa danych.

W związku z powyższym analizy wymaga również proponowany **art. 508a ust. 3**, w którym wskazany został sposób informowania o standardach technicznych i wymaganiach sprzętowych niezbędnych do udziału w zdalnej rozprawie lub zdalnym posiedzeniu. Ze względu na ryzyko dla naruszenia praw lub wolności osób fizycznych, jakie niesie ze sobą przetwarzanie danych z użyciem nowych technologii, przekazywanie tego zapisu do miejsca przebywania osób uczestniczących w zdalnej rozprawie lub zdalnym posiedzeniu powinno odbywać się przy zachowaniu najwyższych standardów technicznych. Prawodawca powinien w treści proponowanych przepisów uwzględnić obowiązki administratora stosownie do art. 32

[6] Dane osobowe muszą być: 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").

rozporządzenia 2016/679[7] i zasad ochrony danych, w sposób odpowiadający celom regulacji. Ponadto, dla realizacji zasady przejrzystości oraz legalizmu (art. 7 Konstytucji RP), standardy techniczne oprogramowania, o których mowa w proponowanym art. 508a ust. 3, określone powinny być w drodze rozporządzenia wykonawczego do ustawy, a nie w drodze obwieszczenia.

Z wyrazami szacunku,

z up. Prezesa Urzędu
Ochrony Danych Osobowych
Zastępczyni Prezesa
Urzędu Ochrony Danych Osobowych
dr hab. Agnieszka Grzelak

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

[7] 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.