Warszawa, 24 czerwca 2022 r.

Szanowny Pan
Janusz Cieszyński
Sekretarz Stanu
w Kancelarii Prezesa Rady Ministrów

Szanowny Panie Ministrze,

W imieniu Związku Cyfrowa Polska branżowej organizacji pracodawców, która zrzesza największe firmy z branży nowoczesnych technologii działające w Polsce, przekładamy stanowisko do ***Projektu ustawy o aplikacji mObywatel*** z dnia 3 czerwca 2022 r.

Na wstępie chcieliśmy pogratulować i wyrazić chęć wsparcia podjętych działań na rzecz rozwoju aplikacji mObywatel. Jesteśmy przekonani, że zaprezentowane w naszym stanowisku uwagi pomogą sprostać oczekiwaniom użytkowników, aby dokumenty elektroniczne obsługiwane przy użyciu tej aplikacji pozwalały na ich wykorzystanie w sposób co najmniej tak szeroki, jak w przypadku odpowiadających im dokumentów tradycyjnych.

Szczegółowe uwagi w formie tabelarycznej odnoszące się do poszczególnych projektowanych zapisów przesyłamy jako załącznik.

Z wyrazami szacunku**,**
Michał Kanownik

Michał Kanownik

Prezes Zarządu
Związek Cyfrowa Polska

Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego - ZIPSEE Cyfrowa Polska

www.zipsee.pl

Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa

Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl

KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

Uwagi **Związku Cyfrowa Polska** do projektu **Ustawy o aplikacji mObywatel**, z dnia 3 czerwca 2022 r.

Przepis projektu ustawy	Uwaga	Dodatkowy komentarz
Art. 1. Ustawa określa zasady funkcjonowania i wykorzystywania publicznego oprogramowania, wykorzystywanego do udostępniania i świadczenia usług, przeznaczonego dla urządzeń mobilnych, zwanego dalej „aplikacją mObywatel", którego użytkownikami są osoby fizyczne.	Ustawa powinna wspierać wykorzystanie mObywatela jako systemu identyfikacji elektronicznej (w przyszłości po wejściu w życie eIDAS2 – portfela tożsamości elektronicznej) w możliwie największym spektrum procesów biznesowych realizowanych przez podmioty prywatne i publiczne. Dla zapewnienia równowagi rynkowej kluczowe jest udostępnienie mObywatel dla wszystkich zainteresowanych interesariuszy (odbiorców identyfikacji elektronicznej), zarówno publicznych jak i prywatnych, na równych zasadach rynkowych. Z uwagi na zapewnienie bezpieczeństwa aplikacji należy ograniczyć możliwość i monitorować migrację aplikacji pomiędzy urządzeniami. W najlepszym przypadku uruchomienie aplikacji mObywatel na nowym urządzeniu powinno wymagać identycznych działań jak rejestracja nowej aplikacji. (ewentualnie przeniesienie na podstawie dedykowanych kodów odzyskiwania, generowanych przy inicjacji aplikacji i nieprzechowywanych w systemie) Aplikacja powinna być jednoznacznie wiązana z urządzeniem, generować zestaw kodów do odzyskiwania/przenoszenia aplikacji (np.. Jak generatory kodów jednorazowych google). W związku z potrzebą zapewnienia najwyższego poziomu bezpieczeństwa i wyjściu naprzeciw oczekiwaniom eIDAS 2.0 zalecane jest użycie modułów kryptograficznych (TPM/TEE/SE) w urządzeniach, na których instalowana będzie aplikacja. Możliwe też może być zmienienie poziomu bezpieczeństwa środka identyfikacji w aplikacji mObywatel w zależności od użycia modułu kryptograficznego. Czy aplikacja będzie przeznaczona tylko na urządzenia mobilne? Będzie możliwość instalacji na komputerach stacjonarnych, lub korzystania przez przeglądarkę? Rozwiązanie takie byłoby również wyjściem naprzeciw wymaganiom eIDAS 2.0.	Dotychczasowa praktyka wykorzystania mObywatel przez strony ufające (odbiorców tożsamości) wskazuje, że jest on udostępniany podmiotom publicznym i selektywnie komercyjnym. Wpływa to na tworzenie przewag konkurencyjnych przez usługodawców mających dostęp do mObywatela. W sposób znaczący zaburza to równowagę rynkową umożliwiając technologiczne i biznesowe subsydiowanie wybranych graczy rynkowych. Dlatego też niezwykle istotne jest udostępnienie mObywatel na równych zasadach wszystkim podmiotom mającym interes faktyczny do korzystania z usługi.
Art. 2. ust. 1. Minister właściwy do spraw informatyzacji udostępnia w aplikacji mObywatel usługi, z których użytkownik tej aplikacji może korzystać przy użyciu urządzenia mobilnego, pozwalające w szczególności na:	Zakres funkcjonalny oraz zakres przetwarzanych danych powinien być spójny z definicjami wprowadzanymi obecnie w ramach eIDAS2. Przepis w projektowanym brzmieniu sugeruje, że wszystkie usługi, z których będzie mógł korzystać obywatel będą świadczone (dostarczane) przez państwo.	mObywatel powinien być w swojej funkcjonalności zbieżny z projektowanym portfelem w eIDAS

Art. 2 ust. 1 pkt. 1) pobranie, przechowywanie, prezentację oraz przekazywanie, przy użyciu urządzenia mobilnego, dokumentu elektronicznego zawierającego dane pobrane z rejestru publicznego lub z systemu teleinformatycznego podmiotu publicznego: a) niezbędne dane osobowe tego użytkownika, b) dane dotyczące sytuacji prawnej tego użytkownika lub praw mu przysługujących, c) dane umożliwiające identyfikację rzeczy związanej z tym użytkownikiem, d) dane dotyczące sytuacji prawnej osoby, której ten użytkownik jest rodzicem lub opiekunem prawnym, lub praw przysługujących tej osobie;	1. Proponowane zapisy zakładają tylko przetwarzanie dokumentów mających swoje źródło w systemach publicznych. W rozporządzeniu eIDAS 2 – źródłem danych mogą być także dostawcy (w tym kwalifikowani) weryfikowalnych poświadczeń (atrybutów). Ci zaś mogą wydawać poświadczenia bazując na zaufanych źródłach danych niekoniecznie publicznych np. dokument potwierdzający zdolność kredytową. 2. Punkty b) – d) są zdefiniowane w eIDAS2 jako elektroniczne atestacje atrybutów. Proponuje się wprowadzenie podobnej definicji i wskazanie b) – d) jako przykładów tych atestacji.	
Art. 2 ust. 1 pkt. 2) przekazanie danych, które zostały pobrane przez użytkownika tej aplikacji z rejestru publicznego lub z systemu teleinformatycznego, innemu podmiotowi świadczącemu usługę w tej aplikacji;	Zawężenie odbiorców danych do podmiotów świadczących usługę „w tej aplikacji" jest znaczącym ograniczeniem. Proponuje się udostępniać dane wszystkim podmiotom mającym interes faktyczny.	
Atr. 2 ust. 1 pkt. 3) identyfikację i uwierzytelnienie w usłudze online udostępnionej przez podmiot publiczny, o którym mowa w art. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070 i 1087);	Ograniczenie stosowania identyfikacji do usług online udostępnianych przez podmioty publiczne jest niezgodne z kierunkiem zmian proponowanych w ramach eIDAS 2.0 oraz zawęża potencjalny zakres zastosowania identyfikacji elektronicznej. Identyfikacja elektroniczna w ramach systemu mObywatel powinna być powszechna i dostępna dla wszystkich podmiotów działających na rynku na jednakowych zasadach.	
Art. 2 ust. 1 pkt. 4) dokonywanie płatności elektronicznych związanych z usługami udostępnianymi w tej aplikacji;	Ponownie – zawężenie do usług udostępnianych w „tej aplikacji". Proponujemy uwolnienie mechanizmu płatności elektronicznych do dowolnych usług, które chcą skorzystać z mechanizmu płatności mObywatel.	
Art. 2 ust. 1 pkt. 5) wykorzystanie urządzenia mobilnego w procesie identyfikacji i uwierzytelnienia w usłudze online jako jednego z czynników uwierzytelniania profilu zaufanego, o którym mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.	Prosimy by rozważyć udostępnienie mechanizmów uwierzytelniania mObywatel na potrzeby świadczenia usług komercyjnych. W szczególnym przypadku mechanizmy te można wykorzystać do aktywacji klucza prywatnego w usłudze składania zdalnego podpisu kwalifikowanego (w szczególności, zgodnie z eIDAS2, będącego jedną z funkcjonalności portfela tożsamości cyfrowej). Czy zasadnym jest używanie jednej aplikacji jako element systemu identyfikacji, do którego następuje uwierzytelnienie oraz jednocześnie generator kodów jednorazowych? Czy takie rozwiązanie było analizowane pod kątem zapewnienia wysokiego poziomu bezpieczeństwa?	
Art. 2 ust. 2. Osoba, której okazywany jest dokument elektroniczny, o którym mowa w ust. 1 pkt 1, dokonuje potwierdzenia autentyczności, ważności, integralności lub pochodzenia tego dokumentu elektronicznego z zastosowaniem wybranych przez siebie procedur, o których mowa w art. 8 ust. 1 pkt 2, i narzędzi, o których mowa w art. 3 ust 1 pkt 4.	Proponujemy doprecyzować zapis „wybranych przez siebie procedur", gdyż obecny może wprowadzać ryzyka bezpieczeństwa. Pozostawienie wyboru użytkownikowi może wpływać na wiarygodność procesu walidacji autentyczności, ważności integralności i źródła pochodzenia. „Algorytm" walidacji powinien zapewniać jej jednoznaczny rezultat dla wszystkich wybranych scenariuszy.	
Art. 2 ust. 5. Dokument elektroniczny, o którym mowa ust. 3, jest dokumentem stwierdzającym tożsamość i obywatelstwo polskie osoby na terytorium	Proponujemy usunąć zapis dotyczący obywatelstwa polskiego. W przypadku Profilu Zaufanego może posiadać go obywatel z zagranicy i wykorzystać do logowania do mObywatela? Czy obcokrajowcy nie będą mogli korzystać z mObywatela?	

Rzeczypospolitej Polskiej, w zakresie danych w nim zawartych, w relacjach wzajemnej fizycznej obecności stron.		
Art. 2 ust. 7. Jeżeli z przepisu prawa wynika obowiązek podania numeru lub serii dokumentu, na podstawie którego stwierdzono obywatelstwo polskie lub tożsamość osoby fizycznej, w przypadku użycia dokumentu, o którym mowa w ust. 3, obowiązek ten uznaje się za spełniony przez podanie numeru i serii dowodu osobistego, zamieszczonego w tym dokumencie, jeżeli dokument zawiera te dane.	Proponujemy odwołać się do pojęć wprowadzonych w Art. 6 eIDAS2, w szczególności zamiast użycia zwrotu „podania danych" proponujemy wykorzystać pojęcie wprowadzane w rozporządzeniu eIDAS2 „prezentacji danych przy zapewnieniu selektywności ich ujawnienia". Prezentacja jest pojęciem bardziej „pojemnym" i obejmuje technicznie możliwość podania danych przez interfejsy: użytkownika (w aplikacji mobilnej) i wymiany danych (API).	
Art. 2 ust. 8. Dokument elektroniczny, o którym mowa w ust. 3, nie może być wykorzystywany do potwierdzenia tożsamości osoby w przypadku, gdy ze względu na cel i skutki prawne potwierdzenia tożsamości poziom pewności i bezpieczeństwa takiego sposobu potwierdzenia tożsamości jest niewystarczający.	Proponowany zapis wskazuje, że aplikacja mObywatel gwarantuje pewien (bliżej nieokreślony) poziom pewności i bezpieczeństwa procesu identyfikacji (LoA – Level of Assurance). Poziom ten jest niewyspecyfikowany w ustawie, w związku z czym strona konsumująca tożsamość, może założyć, z ostrożności, niski poziom wiarygodności środka identyfikacji (LoA low). To może prowadzić do stwierdzenia, że występują przesłanki do odrzucenia tej formy identyfikacji ze względu na cel i skutki prawne. Należy jasno określić poziom wiarygodności tego środka identyfikacji i narzędzi do weryfikacji.	Jeżeli dokument, o którym mowa w ust. 3 ma być odpowiednikiem "tradycyjnego" dowodu osobistego, to powinno być to wyraźnie napisane, że zastępuje on dowód osobisty w każdym przypadku, jeżeli przepisy odrębne nie stanowią inaczej. Jeżeli natomiast nie jest on dokumentem tożsamości na poziomie dowodu osobistego (z ewentualnymi zastrzeżeniami w przepisach odrębnych co do możliwości jego stosowania), to faktycznie należy wprowadzić nową kategorię dokumentu tożsamości (oprócz dowodu i paszportu) z określeniem jego poziomu wiarygodności i zakresu stosowania. W przeciwnym przypadku będzie duży opór akceptacji tego dokumentu przez strony ufające
Art. 2 ust. 9. Rada Ministrów może określić w drodze rozporządzenia przypadki, o których mowa w ust. 8, gdy dokument elektroniczny, o którym mowa w ust. 3, nie może być wykorzystywany do potwierdzenia tożsamości, mając na uwadze wymagania dotyczące poziomu pewności i bezpieczeństwa procesu potwierdzania tożsamości adekwatnie do celu w jakim potwierdzenie tożsamości następuje i skutków prawnych tego potwierdzenia.	Od „czarnej listy" przypadków, w których nie można użyć tego środka identyfikacji lepszym podejściem wydaje się jasne i klarowne określenie jego poziomu pewności i bezpieczeństwa (Level of Assurance), a następnie zbudowanie w drodze rozporządzenia listy przypadków zastosowania różnych środków w zależności od ich poziomu pewności i bezpieczeństwa (low, substantial, high). Takie podejście gwarantuje interoperacyjność z prawodawstwem unijnym.	Ewentualnie jak wyżej
Art. 3 ust. 1 pkt 3) zapewnia bezpieczeństwo oraz integralność danych przekazywanych pomiędzy aplikacją mObywatel, systemem teleinformatycznym, o którym mowa w pkt 2, oraz systemami teleinformatycznymi podmiotów świadczących usługi w tej aplikacji;	Proponujemy zredefiniować pojęcie „podmiotów świadczących usługi w aplikacji". Rozporządzenie eIDAS2 wprowadza pojęcie „relying parties" czyli stron ufających - konsumentów tożsamości. Konsumenci mogą wykorzystywać portfel tożsamości elektronicznej w swoich procesach biznesowych. Usługi te prawdopodobnie nie będą świadczone w „tej aplikacji", a „poza nią". Podstawowy przypadek użycia portfela zgodnego z eIDAS2 zakłada konsumpcję tożsamości przez stronę ufającą bez instalacji/integracji usługi biznesowej „wewnątrz portfela".	
Art. 3 ust. 1 pkt 5) zapewnia, przy użyciu systemu teleinformatycznego, o którym mowa w pkt 2, funkcjonowanie oraz możliwość wykorzystywania i weryfikacji certyfikatu, pozwalającego na:	Ustawa może doprecyzować czy weryfikacja realizowana będzie z uwzględnieniem pryncypium prywatności osoby korzystającej z aplikacji mObywatel (np. CRL, rozpraszanie informacji walidującej w rejestrach rozproszonych), czy umożliwiającej „profilowanie" aktywności obywateli w usługach, z których korzystają np. (dzięki walidacji OCSP). Proponujemy doprecyzować zapis „weryfikacji certyfikatu uwzględniającej prywatność użytkownika, pozwalającego na…".	

Art. 3 ust. 2. Certyfikat, o którym mowa w ust. 1 pkt 5, wydany wraz z dokumentem, o którym mowa w art. 2 ust. 3, zawiera dane użytkownika aplikacji mObywatel: 1) imię (imiona); 2) nazwisko; 3) numer PESEL; 4) numer seryjny certyfikatu.	Proponowana struktura certyfikatu nie sprzyja zapewnieniu prywatności transakcji identyfikacji zawieranych przy użyciu mObywatel i umożliwia „profilowanie" aktywności obywateli na postawie danych zawartych w certyfikacie (przez potencjalnych adwersarzy). Dane walidujące podpisy i pieczęci (klucz publiczny) nie powinny być związane z tożsamością osoby fizycznej. Już sam klucz publiczny może być traktowany jako unikalny identyfikator osoby fizycznej, umożliwiający jej profilowane. Dlatego należy zastanowić się nad metodami walidacji gwarantującymi prywatność obywateli np. wspomnianymi w eIDAS2 metodami bazującymi na ZKP/ZKA. Zgodnie z aktualnym brzmieniem eIDAS2: „In addition, ZKP could help fight against bots and disinformation attacks, as platforms could verify that an action on their platform (content, vote, comment, etc.) is executed by a real person located in the Union, while preserving the right to anonymity. W przypadkach, w których śledzenie aktywności obywateli jest niepożądane rekomendujemy walidowanie przy pomocy metod ZKP.	
Art. 3 ust. 3. Certyfikat, o którym mowa w ust. 1 pkt 5, wydany wraz z mLegitymacją szkolną, o której mowa w art. 11 ust. 1b ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2021 r. poz. 1915 oraz z 2022 r. poz. 583 i 1116), lub z mLegitymacją studencką, o której mowa w art. 74 ust. 4a ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2022 r. poz. 574, 582, 665, 682, 682, 807, 1010, 1079 i 1117), zawiera dane użytkownika aplikacji mObywatel: 1) imię (imiona); 2) nazwisko; 3) numer PESEL; 4) numer seryjny certyfikatu; numer identyfikujący legitymację.	Uwaga: jak w przypadku ust. 2.	
Art. 4 ust. 1 pkt. 2) złożyła wniosek o wydanie dowodu osobistego, a jej tożsamość i obywatelstwo zostały potwierdzone w sposób, o którym mowa w art. 29a ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2022 r. poz. 671).	Aby posiadać numer PESEL i PZ nie jest wymagane obywatelstwo PL. Dlaczego działanie mObywatela ma być ograniczone tylko dla obywateli PL? Czy na pewno wystarczy złożenie wniosku o wydanie DO? Jeśli będzie rozpatrzony negatywnie, to co z aplikacją mObywatel?	
Art. 4 ust. 3. Użytkowanie aplikacji mObywatel jest bezpłatne i dobrowolne. Użytkownik aplikacji mObywatel może w dowolnej chwili zrezygnować z korzystania z tej aplikacji.	Niezwykle istotny zapis. Popieramy jego brzmienie i sugerujemy „podniesienie" tego ustępu do rangi artykułu.	

	Możliwość rezygnacji ze środka identyfikacji elektronicznej i realizacji usług w formie dotychczasowej/klasycznej jest jednym ze scenariuszy obsługi incydentu kompromitacji środka.	
Art. 4 ust. 4. Użytkownik aplikacji mObywatel, o którym mowa w ust. 1, może przy użyciu tej aplikacji oraz systemu teleinformatycznego, o którym mowa w art. 3 ust. 1 pkt 2, pobrać, na potrzeby wykorzystywanej usługi, z:	Proponujemy przenieść rejestr dokumentów do rozporządzenia.	
Art. 4 ust. 6. Minister właściwy do spraw informatyzacji zapewnia możliwość unieważnienia certyfikatu, o którym mowa w art. 3 ust. 1 pkt 5, w szczególności w przypadku utraty przez użytkownika aplikacji mObywatel kontroli nad tą aplikacją.	Parametry kluczowe dla procesu unieważnienia informacji służącej do walidacji (certyfikatów) powinny być doprecyzowane (na poziomie rozporządzenia). Są one kluczowe dla bezpieczeństwa systemu identyfikacji. Przykładowo: czas publikacji informacji o unieważnieniu od momentu zgłoszenia incydentu przez obywatela – 24godziny. Czas ten może wpływać na „niepewność" procesu walidacji tożsamości (np. w ciągu 24h może zostać zaktualizowana informacja o unieważnieniu). Wpływa to ogólnie/makroekonomicznie na niepewność transakcji zawieranych elektronicznie (im krótszy czas obsługi procesów unieważniania, tym ryzyka bezpieczeństwa niższe).	
Art. 5. ust. 1. Minister właściwy do spraw informatyzacji może określić standard świadczenia usługi udostępnianej w aplikacji mObywatel.	1.Należy zagwarantować równe zasady dostępu do usługi przez podmioty publiczne i prywatne. Zapobiegnie to tworzeniu przewag konkurencyjnych przez wybranych interesariuszy rynkowych. 2. Rozporządzenie eIDAS wiąże usługi identyfikacji z usługami zaufania. Tylko połączenie tych dwóch ekosystemów tworzy spójny system bezpieczeństwa będący pod nadzorem Państwa. Rekomendujemy wskazanie explicite dostawców usług zaufania jako domyślnego konsumenta usług identyfikacji. Umożliwi to jawne wskazanie „bezpiecznego łańcucha dostaw" usług dla obywateli. 3. Rekomendujemy wskazanie w ramach pkt. 3 „warunki organizacyjne i techniczne" SLA dla usługi mObywatel. Bez wskaźników dostępności mObywatel utrudniona może być adopcja tego środka w procesach biznesowych świadczonych przez podmioty komercyjne świadczące usługi dla klientów zgodnie ze zdeklarowaną przez nie dostępnością.	
Art. 5. ust. 3. Podmiot może świadczyć w aplikacji mObywatel usługę, dla której minister właściwy do spraw informatyzacji określił standard świadczenia usługi, na podstawie wniosku złożonego do ministra właściwego do spraw informatyzacji.	Bardzo nieprecyzyjny zapis dający duże pole interpretacji i nadużyć oraz potencjalnie sterowanie rynkiem odbiorców usług identyfikacji. Niedobrym byłoby wymuszenie świadczenie usług przez tzw. „relying parties" (konsumentów tożsamości) tyko „w aplikacji mObywatel" zgodnie z bliżej nieokreślonym standardem świadczenia usługi. Dlatego też niezwykle ważne jest wskazanie, że możliwe jest zintegrowanie z aplikacją mObywatel i świadczenie usług poza aplikacją.	
Art. 6 ust. 1. pkt. 3) dostępność zasobów technicznych, osobowych oraz finansowych, jakimi dysponuje urząd obsługujący tego ministra, jednostki mu podległe i przez niego nadzorowane, warunkujących możliwość świadczenia wnioskowanej usługi;	Ten punkt jawnie wskazuje, że udostępnienie w aplikacji mObywatel nowej usługi jest możliwe tylko dla urzędów publicznych. Rekomendujemy zmianę zapisów, aby: a) Aplikacja mObywatel była otwarta dla prywatnych dostawców usług chcących je	

	świadczyć w aplikacji mObywatel b) Aplikacja mObywatel była otwarta dla prywatnych dostawców usług chcących konsumować tożsamość („relying parties") poza aplikacją mObywatel (z wykorzystaniem interfejsu wymiany danych, API).	
Art. 6 ust. 1. pkt. 5) pierwszeństwo w udostępnianiu usług podmiotów publicznych.	Zapis preferujący publicznych graczy rynkowych zaburzający równowagę i równe zasady konkurencji.	
Art. 7. Minister właściwy do spraw informatyzacji przetwarza w systemie teleinformatycznym, o którym mowa w art. 3 ust. 1 pkt 2, dane osobowe użytkowników aplikacji mObywatel w zakresie niezbędnym do realizacji usług udostępnionych w tej aplikacji, a także w celu zapewnienia bezpieczeństwa teleinformatycznego i bezpieczeństwa obrotu prawnego. Dane osobowe przetwarzane są przez ministra właściwego do spraw informatyzacji przez okres 6 lat od dnia ostatniej aktywności użytkownika aplikacji mObywatel, którego te dane dotyczą.	Brak określenia zakresu danych przetwarzanych w zakresie niezbędnym do świadczenia usług poza aplikacją mObywatel przez konsumentów usługi identyfikacji „relying parties" (np. adresów IP systemów konsumujących tożsamość).	
Art. 8. ust. 1. Minister właściwy do spraw informatyzacji, w Biuletynie Informacji Publicznej na swojej stronie podmiotowej, udostępnia oraz niezwłocznie aktualizuje informacje o:	Rekomendujemy dodanie zapisu wskazującego, że informacja będzie udostępniana w formacie umożliwiającym przetwarzanie maszynowe.	