UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie delegacji zawartej w art. 13 ustawy   
z dnia 6 grudnia 2018 r. o Krajowym Rejestrze Zadłużonych (Dz. U. z 2019 r. poz. 55, 912, 1214 i 1802 oraz z 2020 r. poz. 1747), zwanej dalej „ustawą”. Zgodnie z tym przepisem Minister Sprawiedliwości określi, w drodze rozporządzenia, sposób przetwarzania danych zawartych w Krajowym Rejestrze Zadłużonych, w tym również danych, o których mowa w art. 11 ust. 1 ustawy mając na uwadze potrzebę zapewnienia czytelności oraz przejrzystości danych prezentowanych w Rejestrze, łatwość jego użytkowania oraz konieczność zapewniania bezpieczeństwa przetwarzanych danych.

W § 1 rozporządzenia określa zakres przedmiotowy rozporządzenia.

W § 2 określono sposób zamieszczania danych w Rejestrze. Zasadą jest, że dane będą zamieszczane w Rejestrze za pośrednictwem Systemu teleinformatycznego. Przy czym projekt przewiduje również możliwość zamieszczania danych bezpośrednio przez system teleinformatyczny organu uprawnionego do zamieszczania danych określonych w art. 7 i 8 ustawy. Celem tej regulacji jest umożliwienie zamieszania danych w Rejestrze w sposób automatyczny poprzez przesył danych z systemu teleinformatycznego organu uprawnionego do zamieszczania tych danych.

Organem uprawnionym do zamieszczania danych określonych w art. 7 i 8 ustawy jest w szczególności komornik sądowy, sąd, Szef Krajowej Administracji Skarbowej, naczelnik urzędu skarbowego, dyrektor oddziału Zakładu Ubezpieczeń Społecznych oraz organ, który wypłacił świadczenia przyznawane w przypadku bezskuteczności egzekucji alimentów.

W § 3 określono miejsce udostępniania danych zawartych w Rejestrze oraz kryteria wyszukiwania tych danych. Zgodnie z projektowanym § 3 ust. 1 w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego Ministra Sprawiedliwości można zapoznać się z danymi ujawnionymi w Rejestrze. Przepis ten realizuje zasadę jawności Rejestru. Zasada ta została przez ustawodawcę wyrażona w art. 4 ustawy. Zgodnie z tym przepisem każdy ma prawo zapoznać się z danymi ujawnionymi w Rejestrze oraz danymi objętymi treścią obwieszczeń za pośrednictwem sieci Internet. Dla realizacji funkcji Rejestru istotne jest takie określenie kryteriów wyszukiwania danych ujawnionych w Rejestrze, aby – po pierwsze dostęp do danych był łatwy, po drugie – wyszukanie miało charakter pewny.

W stosunku do osób fizycznych, które nie prowadzą działalności gospodarczej kryterium wyszukiwania danych ujawnionych w Rejestrze w zakresie postępowania upadłościowego, restrukturyzacyjnego oraz bezskuteczności egzekucji jest numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), numer identyfikacji podatkowej (NIP) albo sygnatura akt sprawy.

W stosunku do osób fizycznych, które prowadzą działalność gospodarczą kryterium wyszukiwania danych ujawnionych w Rejestrze w zakresie postępowania upadłościowego, restrukturyzacyjnego oraz bezskuteczności egzekucji jest imię i nazwisko, firma, numer PESEL, NIP albo sygnatura akt sprawy. W stosunku do tych podmiotów rozszerzenie kryterium wyszukiwania danych ujawnionych w Rejestrze jest uzasadnione tym, że podmioty te w obrocie gospodarczym występują pod imieniem i nazwiskiem oraz firmą. Jeżeli Rejestr ma wzmocnić bezpieczeństwo obrotu gospodarczego to w stosunku do tych podmiotów dostęp do ujawnionych danych w Rejestrze powinien być możliwy przy zastosowaniu wskazanych kryteriów.

W stosunku do podmiotów niebędących osobami fizycznymi kryterium wyszukiwania danych ujawnionych w Rejestrze w zakresie postępowania upadłościowego, restrukturyzacyjnego oraz bezskuteczności egzekucji jest nazwa lub firma, numer w Krajowym Rejestrze Sądowym (KRS), NIP albo sygnatura akt sprawy.

Jeżeli dane zawarte w Rejestrze dotyczą składnika i stanu masy upadłości kryterium wyszukiwania zostało rozszerzone o typ składnika masy upadłości, część opisu bądź nazwy składnika masy upadłości, wartość oszacowania, status składnika masy upadłości, numer składnika masy upadłości ze spisu inwentarza oraz wskazanie podmiotu pełniącego funkcję syndyka masy upadłości. Powyższe rozwiązanie realizuje założenie ustawy w zakresie transparentności zarządzania majątkiem upadłego oraz zwiększa efektywność sprzedaży prowadzonej przez syndyka masy upadłości, bowiem ustawa wprowadza rozwiązanie, zgodnie z którym, syndyk masy upadłości dokonując sprzedaży składników tej masy winien niezwłocznie ujawniać sprzedaż w Rejestrze. Oznacza to, że syndyk masy upadłości lub osoby, które na zlecenie jego zajmują się likwidacją masy upadłości powinny dokonując sprzedaży rejestrować fakt sprzedaży w Rejestrze. Obowiązek taki jest odzwierciedleniem na gruncie postępowania upadłościowego działań rynkowych systemów sprzedażowych, które opierają się na założeniu, że każdorazowy fakt sprzedaży jest odnotowywany w systemie magazynowym. Takie rozwiązanie pozwoli wierzycielom na bieżące śledzenie postępów likwidacji masy upadłości, a potencjalnym nabywcom zagwarantuje dostęp do zawsze aktualnych informacji o składnikach majątku przeznaczonych do sprzedaży.

W stosunku do osób fizycznych, które są dłużnikami alimentacyjnymi, kryterium wyszukiwania danych ujawnionych w Rejestrze jest numer PESEL.

W projekcie przyjęto rozwiązanie, że w sytuacji braku numeru PESEL kryterium wyszukiwania (czyli inną daną umożliwiającą identyfikację osoby fizycznej, której dane zostały ujawnione w Rejestrze) w szczególności jest numer paszportu i oznaczenie państwa wystawiającego paszport albo numer karty pobytu w Rzeczypospolitej Polskiej albo zagraniczny numer identyfikacji lub identyfikacji podatkowej. Natomiast w stosunku do podmiotu niebędącego sobą fizyczną przyjęto rozwiązanie, że w przypadku braku numeru KRS kryterium wyszukiwania (czyli inną daną umożliwiającą identyfikację tego podmiotu, którego dane zostały ujawnione w Rejestrze) w szczególności jest numer w zagranicznym rejestrze albo zagraniczny numer identyfikacji lub identyfikacji podatkowej.

Zgodnie z art. 2 ust. 2 ustawy, jeżeli przepis szczególny tak stanowi, w Rejestrze dokonuje się również obwieszczeń dotyczących informacji o postępowaniach upadłościowych oraz restrukturyzacyjnych. W konsekwencji w § 4 projektowanego rozporządzenia uregulowano, że obwieszczeń w Rejestrze dokonuje się za pośrednictwem Systemu teleinformatycznego.

W § 5 ust. 1 określono sposób przekazywania do celów statystycznych danych, których ujawniania zaprzestano poprzez wskazanie podmiotu, który w ramach Ministerstwa Sprawiedliwości opracowuje dane w celu dalszego udostępnienia w celach statystycznych.   
W ust. 2 określono sposób, w jaki ww. dane będą przekazywane komórce Ministerstwa Sprawiedliwości oraz zakres czynności poprzedzających przekazanie danych do celów statystycznych (kontrola kompletności i jakości danych).

W § 6 ust. 1 projektowanego rozporządzenia określono warunki, tryb i sposób przekazywania danych, których ujawniania zaprzestano do badań naukowych. Wskazano, że dane te są udostępniane wyłącznie na wniosek oraz przekazywane przez Ministra Sprawiedliwości, gdyż zgodnie z art. 1 ustawy to Minister Sprawiedliwości prowadzi Rejestr. Natomiast art. 12 ust. 2 ustawy stanowi, że Minister Sprawiedliwości jest administratorem danych zgromadzonych w Rejestrze oraz danych objętych treścią obwieszczeń.

Przekazanie danych powinno nastąpić w terminie 30 dni od dnia otrzymania wniosku. Przy czym jest to termin o charakterze instrukcyjnym.

W § 6 ust. 2 określono szczegółowe wymagania formalne dla wniosku o przekazanie danych do celów naukowych. Zgodnie z tym przepisem wniosek musi zawierać zwięzły opis celów badawczych oraz programu badań, zakres żądania danych wraz   
z uzasadnieniem oraz informacje umożliwiające wyszukanie żądanych danych w zbiorze. Powyższe warunki przekazywania danych do badań naukowych pozwolą na weryfikację czy żądanie danych faktycznie następuje do celów naukowych oraz czy zakres żądanych danych pokrywa się z zakresem prowadzonych badań.

Zgodnie z ust. 3 odmowa udostępnienia danych, których ujawniania zaprzestano do badań naukowych wymaga uzasadnienia.

Z uwagi na to, że ustawa wchodzi w życie z dniem 1 grudnia 2021 r. koniecznym jest, aby z tą datą weszło w życie przedmiotowe rozporządzenie.

Przetwarzanie danych osobowych w Rejestrze oparte jest na art. 6 ust. 1 lit c) i e) rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (dalej: RODO). Oznacza to, że przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze oraz przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa przetwarzania, o której mowa w art. 6 ust. 1 lit. c) i e) RODO, określona jest w ustawie.

Artykuł 4 ustawy określa, że Rejestr jest jawny i każdy ma prawo zapoznać się z danymi ujawnionymi w Rejestrze oraz danymi objętymi treścią obwieszczeń za pośrednictwem sieci Internet. Zgodnie z art. 5 ustawy przetwarzane dane osobowe obejmują numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) albo numer w Krajowym Rejestrze Sądowym, a w przypadku ich braku – inne dane umożliwiające jednoznaczną identyfikację, w szczególności numer paszportu i oznaczenie państwa wystawiającego paszport albo numer karty pobytu w Rzeczypospolitej Polskiej, albo numer w zagranicznym rejestrze, albo zagraniczny numer identyfikacji lub identyfikacji podatkowej.

W związku z powyższym istotne jest zapewnianie bezpieczeństwa przetwarzanych danych osobowych zgromadzonych w Rejestrze.

Zabezpieczenie tych danych będzie realizowane z uwzględnieniem zasad wynikających z art. 25 RODO – Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych. Zasady te nakładają na administratora obowiązek, aby – 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 zagrożenia wynikające z przetwarzania – wdrażał, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, 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. W związku z tym wdrożone zostały 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.

W ramach zabezpieczeń technicznych wdrożono:

1. Szyfrowanie komunikacji, w szczególności komunikacji prowadzonej via sieć Internet,
2. Proces testów bezpieczeństwa w tym testów penetracyjnych,
3. Separacje sieci,
4. Monitorowanie, audyt zdarzeń,
5. Okresowe przeglądy i audyty Systemu,
6. Ochrona przed złośliwym oprogramowaniem, system klasy EDR,
7. Proces zarządzania podatnościami, aktualizacja oprogramowania,
8. Separacja kont administracyjnych od kont użytkownika,
9. Możliwość aktualizacji metryk uczestników postępowania,
10. Możliwość weryfikacji danych w rejestrach urzędowych np. PESEL, KRS, CRP KEP,
11. Testy oprogramowania w zakresie zgodności ujawnianych danych na stronie z ustawą,
12. Testy bezpieczeństwa, w tym testy penetracyjne,
13. Oddzielenie kont administracyjnych od kont użytkownika,
14. Separacja danych publicznych od systemu prowadzenia postepowań,
15. Uprawnienia statyczne, uprawnienie do danych, Cerber,
16. Użytkownik wewnętrzny – integracja z mechanizmami bezpieczeństwa AD w Ministerstwie,
17. Użytkownik zarejestrowany – wykorzystanie 2FA (RedHat SSO),
18. Wprowadzane w systemie hasła nie są pokazywane na monitorze otwartym tekstem,
19. Konieczność uwierzytelnienie się inną metodą niż hasło podczas operacji zmiany danych w MT,
20. Wykorzystanie 2FA (RedHat SSO),
21. Zastosowanie filtrów prywatyzacyjnych,
22. Odpowiednie ustawienie monitorów,
23. Odpowiednie ustawienie kamer CCTV,
24. Stosowanie wygaszacza ekranu. Wymaganie hasła do odblokowania wygaszacza ekranu,
25. Automatyczne blokowanie ekranu w wyniku bezczynności użytkownika,
26. Ochrona przed złośliwym oprogramowaniem, system klasy EDR,
27. System kontroli dostępu oraz monitoringu wizyjnego,
28. Zgłaszanie naruszeń do Urzędu Ochrony Danych Osobowych,
29. Logiczny model dziedziny i fizyczny model danych – uzgodniony i zatwierdzony przez Ministerstwo,
30. Testy oprogramowania,
31. Complaince – proces zarzadzania zgodnością z przepisami prawa,
32. Szyfrowanie nośników wymiennych,
33. Blokowanie portów USB na stacjach roboczych,
34. Zakazy proceduralne stosowania prywatnych nośników oraz jasno określone zasady naruszenia odpowiedzialności dyscyplinarnej,
35. Rozwiązanie klasy SIEM,
36. Proces zarządzania logami, retencja logów,
37. Eliminacja pojedynczych punktów awarii,
38. Redundancja, Klastrowanie, OpenShift,
39. Przegląd i konserwacja urządzeń infrastruktury,
40. Agregaty prądotwórcze, ups,
41. Zabezpieczenia w warstwie sieciowej ITS (Firewall, IDS/IPS, separacja sieci),
42. Szyfrowanie komunikacji, w szczególności via sieć Internet,
43. Szyfrowanie danych (w spoczynku, w ruchu, procesowanych),
44. Strategia „ochrony w głąb”,
45. Procedura kopii bezpieczeństwa,
46. Testowe odtwarzanie kopii bezpieczeństwa i weryfikacja systemu po odtworzeniu,
47. Klimatyzacja precyzyjna,
48. System p-poż,
49. Oświetlenie awaryjne,
50. Drzwi antywłamaniowe odpowiedniej klasy,
51. Podłoga techniczna,
52. System kontroli dostępu,
53. System monitoringu wizyjnego,
54. Całodobowa ochrona fizyczna,
55. Umowy na dostawy usług,
56. Zarządzanie konfiguracją – skany infrastruktury.

W ramach zabezpieczeń organizacyjnych wdrożono:

1. Proces zarządzania uprawnieniami i upoważnieniami do przetwarzania danych osobowych,
2. Szkolenia i podnoszenia świadomości użytkowników Systemu,
3. Zasady czystego biurka,
4. Zasady czystego ekranu,
5. Zasady minimalnych uprawnień,
6. Procedury postępowania z dokumentacją,
7. Obsługę incydentów,
8. Zgłaszanie naruszeń do Urzędu Ochrony Danych Osobowych,
9. Możliwość aktualizacji metryk uczestników postępowania,
10. Możliwość złożenia i przetwarzania dokumentów wymaganych przez przepisy prawa,
11. Analizę danych osobowych przetwarzanych w systemie pod kątem konieczności zawarcia umów powierzenia przetwarzania danych osobowych,
12. Analiza przetwarzanych danych osobowych w Systemie pod kątem spełnienia wymagań wynikających z art. 6 ust. 1 lit a) RODO,
13. Klauzule informacyjne dostarczone przez Ministerstwo,
14. Analizę przetwarzanych danych osobowych w Systemie pod kątem spełnienia wymagań wynikających z art. 15–22 RODO,
15. Implementację zasad zaprzestania ujawniania informacji zgodnie z ustawą,
16. Zgłaszanie nowych czynności przetwarzania do Rejestru Czynności Przetwarzania Danych.

Bezpieczeństwo danych osobowych będzie również realizowane poprzez precyzyjne określenie kryteriów wyszukiwania podmiotu w Rejestrze, aby – po pierwsze była to informacja łatwo dostępna, po drugie – wyszukanie miało charakter pewny. Kryteriami takimi są m.in. numery identyfikacyjne NIP, PESEL. W odniesieniu do osób fizycznych jedynie numer PESEL jest pewnym i jednoznacznym identyfikatorem. Wskazanie numeru PESEL pozwoli w sposób szybki i łatwy ustalić, czy dana osoba figuruje w Rejestrze. Zastosowanie innego identyfikatora np. imienia i nazwiska, choć dopuszczalne – może skutkować uzyskaniem kilkunastu lub nawet kilkudziesięciu wyników wyszukiwania, a zatem uzyskaniem informacji o zupełnie innych osobach, którymi wyszukujący nie jest zainteresowany. Podanie numeru PESEL służy również ochronie danych innych osób ujawnionych w Rejestrze. Innymi słowy zapewnienia się bezpieczeństwo przetwarzanych danych osobowych przy jednoczesnej realizacji zasady ochrony obrotu prawnego oraz przy jednoczesnej realizacji transparentności postępowań upadłościowych oraz postępowań restrukturyzacyjnych.

Bezpieczeństwo przetwarzania danych osobowych w Rejestrze reguluje również następująca dokumentacja bezpieczeństwa:

1. Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości,

2. Polityka Bezpieczeństwa Systemu Teleinformatycznego Krajowego Rejestru Zadłużonych,

3. Procedury obsługi incydentów,

4. Polityka Bezpieczeństwa Danych Osobowych Ministerstwa Sprawiedliwości,

5. Regulamin Użytkownika Systemów Teleinformatycznych,

6. Procedura nadawania uprawnień w systemie.

Dopełnieniem zapewnienia bezpieczeństwa przetwarzania danych osobowy w Rejestrze jest wprowadzenie następujących mechanizmów:

1. Zaimplementowano klauzule informacyjne dostarczone przez Ministerstwo Sprawiedliwości,
2. Realizacja uprawnień wynikających z art. 15-22 RODO odbywa się na podstawie przepisów ustawy, z uwzględnieniem wyłączeń wynikających z art. 175dc § 2 ustawy z dnia 27 lipca 2001 r. o Ustroju sądów powszechnych (tj. Dz.U. z 2020 r. poz. 2072),
3. Przed wdrożeniem produkcyjnym systemu czynności przetwarzania związane z Krajowym Rejestrem Zadłużonych zostały uwzględnione w Rejestrze czynności przetwarzania danych w Ministerstwie Sprawiedliwości,
4. W Systemie Krajowego Rejestru Zadłużonych, zaimplementowano funkcjonalność, która pozwala na zaprzestanie ujawniania informacji zgodnie   
   z ustawą.
5. Na etapie przygotowania postępowania o udzielenie zamówienia publicznego przeprowadzono analizę pod kątem obowiązku zawarcia umowy powierzenia danych osobowych. Umowa została zawarta,
6. Komunikacja pomiędzy przeglądarką a serwerem front-end odbywa się z wykorzystaniem bezpiecznego, zaszyfrowanego kanału,
7. Na etapie odbioru oprogramowania przeprowadzone zostały testy bezpieczeństwa, w tym testy penetracyjne,
8. Wdrożono mechanizmy logowania zdarzeń w Systemie Krajowego Rejestru Zadłużonych,
9. Każdy administrator posiada imienne konto administracyjne oraz imienne konto zwykłego użytkownika do realizacji zadań niewymagających uprzywilejowanego dostępu,
10. Przeprowadzono przedwdrożeniowy audyt bezpieczeństwa systemu Krajowego Rejestru Zadłużonych,
11. W Systemie Krajowego Rejestru Zadłużonych regularnie wykonywane oraz testowane są kopie zapasowe,
12. Architektura Systemu Krajowego Rejestru Zadłużonych minimalizuje występowania pojedynczych punktów awarii,
13. Zaplanowano przeprowadzenie szkoleń przedwdrożeniowych i powdrożeniowych,
14. Zabezpieczenia serwerowni gwarantują bezpieczną eksploatację centralnego systemu teleinformatycznego Krajowego Rejestru Zadłużonych,
15. System Krajowego Rejestru Zadłużonych umożliwia użytkownikom zarejestrowanym włączenie mechanizmu uwierzytelnienia dwuskładnikowego,
16. Przeprowadzono proces testów akceptacyjnych, potwierdzających zgodność Systemu Krajowego Rejestru Zadłużonych z wymaganiami Ministerstwa Sprawiedliwości,
17. Zaimplementowany w Systemie Krajowego Rejestru Zadłużonych logiczny model dziedziny oraz fizyczny model danych umożliwia przetwarzanie danych tyko na potrzeby ustawy,
18. Wprowadzono separację danych, na poziomie schematu bazy danych, które mają być dostępne publicznie od danych na etapie prowadzenia postępowania.

Rozporządzenie nie wykonuje prawa Unii Europejskiej.

Rozporządzenie nie zawiera przepisów technicznych, a zatem nie podlega notyfikacji zgodnie z trybem przewidzianym w rozporządzeniu Rady Ministrów z dnia 23 grudnia   
2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597). Projekt rozporządzenia został zamieszczony w Biuletynie Informacji Publicznej na stronach Rządowego Centrum Legislacji, stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Projekt nie podlega zaopiniowaniu przez właściwe instytucje i organy Unii Europejskiej ani przez Europejski Bank Centralny.