Instytut Wymiaru Sprawiedliwości

Rozwiązania legislacyjno-organizacyjne zapewniające udostępnienie danych w poszczególnych rejestrach publicznych (w tym w aktach rejestrowych) w trybie ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, ze szczególnym uwzględnieniem rozwiązań mających na celu zapewnienie ochrony danych osobowych

dr Krzysztof Świtała

Prawa podstawowe
Warszawa 2024

Spis treści

1. **Rejestry podlegające analizie** 5
2. **Ochrona danych osobowych w kontekście rejestrów zarządzanych przez Ministerstwo Sprawiedliwości** 7
3. **W jakim zakresie organy publiczne powinny udostępniać dane z rejestrów publicznych oraz akt rejestrowych przez API i jak zapewnić przy tworzeniu API ochronę danych osobowych?** 9
4. **W jakim zakresie organy publiczne powinny udostępniać dane z rejestrów publicznym i akt rejestrowych na wniosek, z uwzględnieniem ochrony danych osobowych?** 21
5. **Czy możliwe jest ustalenie w prawie krajowym dodatkowych wymogów dotyczących wniosku, np. wymogu złożenia go przez system teleinformatyczny w postaci elektronicznej?** 23
6. **Czy fakt jednoczesnej dostępności danych w publicznym rejestrze uzasadnia w świetle przepisów Unii Europejskiej odmowę uwzględnienia wniosku o ich udostępnienie?** 24
7. **Krótka charakterystyka toczących się lub planowanych prac legislacyjnych związanych z tematem badawczym** 25

Bibliografia 26

1. Rejestry podlegające analizie

Rejestry sądowe i administracyjne zarządzane przez Ministerstwo Sprawiedliwości, ze wskazaniem podstaw prawnych do ich prowadzenia:

1) Krajowy Rejestr Sądowy – ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym[1] (https://wyszukiwarka-krs.ms.gov.pl/),
2) Krajowy Rejestr Karny – ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym[2] (ekrk.ms.gov.pl),
3) Księgi Wieczyste – ustawa z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece[3] (ekw.ms.gov.pl).
4) Rejestr Zastawów – ustawa z dnia 6 grudnia 1996 r. o zastawie rejestrowym i rejestrze zastawów[4],
5) Krajowy Rejestr Zadłużonych – ustawa z dnia 6 grudnia 2018 r. o Krajowym Rejestrze Zadłużonych[5] (krz.ms.gov.pl) – w tym: Lista Doradców Restrukturyzacyjnych;
6) Rejestr Sprawców Przestępstw na Tle Seksualnym – rozdział 2 „Rejestr Sprawców Przestępstw na Tle Seksualnym" ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich[6] (rps.ms.gov.pl),
7) Rejestr Funduszy Inwestycyjnych – ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi[7]. Sposób prowadzenia rejestru funduszy inwestycyjnych reguluje rozporządzenie Ministra Sprawiedliwości z dnia 19 grudnia 2016 r. w sprawie rejestru funduszy inwestycyjnych[8],

[1] Tekst jedn. Dz.U. z 2024 r. poz. 979.
[2] Tekst jedn. Dz.U. z 2024 r. poz. 276.
[3] Tekst jedn. Dz.U. z 2023 r. poz. 1984 ze zm.
[4] Tekst jedn. Dz.U. z 2018 r. poz. 2017.
[5] Tekst jedn. Dz.U. z 2021 r. poz. 1909.
[6] Tekst jedn. Dz.U. z 2024 r. poz. 560 ze zm.
[7] Tekst jedn. Dz.U. z 2024 r. poz. 1034.
[8] Dz.U poz. 2188.

8) Rejestr Funduszy Emerytalnych – ustawa z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych[9],
9) Lista tłumaczy przysięgłych – art. 6 ust. 2 ustawy z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego[10],
10) Wykaz postępowań grupowych – art. 11a ust. 1 ustawy z dnia 17 grudnia 2009 r. o dochodzeniu roszczeń w postępowaniu grupowym[11] (www.gov.pl/web/sprawiedliwosc/wykaz-postepowan-grupowych),
11) Lista komorników sądowych – art. 8 ust. 7 ustawy z dnia 22 marca 2018 r. o komornikach sądowych[12] (www.gov.pl/web/sprawiedliwosc/znajdz-komornika-sadowego),
12) Rejestr instytucji kultury, których organizatorem jest Minister Sprawiedliwości – zbiór prowadzony na podstawie zarządzenia Ministra Sprawiedliwości z dnia 8 czerwca 2020 r. w sprawie utworzenia rejestru instytucji kultury, których organizatorem jest Minister Sprawiedliwości[13], w oparciu o art. 14 ust. 1 ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej[14].

Moduł „Elektroniczny dostęp do Sądów Rejestrowych/Centralnej Informacji/Monitora Sądowego i Gospodarczego" umożliwia:

1) składanie i przesyłanie drogą elektroniczną wniosków, załączników i dokumentów do sądów rejestrowych lub Centralnej Informacji Rejestru Zastawów;
2) odbieranie korespondencji z sądów i Centralnej Informacji Rejestru Zastawów.

Zaprezentowany powyżej wykaz pozwoli na czytelne przywoływanie poszczególnych rejestrów w dalszej części niniejszego opracowania.

[9] Tekst jedn. Dz.U. z 2024 r. poz. 1113.
[10] Tekst jedn. Dz.U. z 2019 r. poz. 1326.
[11] Tekst jedn. Dz.U. z 2023 r. poz. 1212 ze zm.
[12] Tekst jedn. Dz.U. z 2023 r. poz. 1691 ze zm.
[13] Dz.Urz. Min. Spr. z 2020 r. poz. 136.
[14] Tekst jedn. Dz.U. z 2024 r. poz. 87.

2. Ochrona danych osobowych w kontekście rejestrów zarządzanych przez Ministerstwo Sprawiedliwości

Z punktu widzenia ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego[15] zgodnie z art. 7 ust. 1 przepisy ustawy nie naruszają prawa dostępu do informacji publicznej ani wolności jej rozpowszechniania, ani przepisów innych ustaw określających zasady, warunki i tryb dostępu lub ponownego wykorzystywania informacji będących informacjami sektora publicznego. Na podstawie zaś art. 7 ust. 2 u.o.d.p.w. przepisy ustawy nie naruszają przepisów o ochronie danych osobowych.

Zgodnie z art. 6 ust. 2 u.o.d.p.w. dostęp do informacji podlega ograniczeniu ze względu na tajemnicę przedsiębiorstwa lub prywatność osoby fizycznej, w tym ochronę danych osobowych. W dalszej części opracowania zostaną przeanalizowane najistotniejsze wątki związane ze wspomnianą limitacją rzeczonych uprawnień.

Ogólne rozporządzenie o ochronie danych (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[16]) ma zastosowanie do wszelkich form przetwarzania danych w rejestrach będących w gestii Ministerstwa Sprawiedliwości (z wyłączeniem Krajowego Rejestru Karnego). Zgodnie z art. 2 ust. 1 RODO: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych". W odniesieniu do rejestrów publicznych oznacza to, że bez względu na postać przetwarzania danych przepisy tego aktu prawa Unii Europejskiej znajdują zastosowanie.

Co do zasady w kontekście zasobów informacyjnych zarządzanych przez Ministerstwo Sprawiedliwości stosujemy RODO. Należy jednak zaznaczyć, że są od tego wyjątki, zgodnie

[15] Tekst jedn. Dz.U. z 2023 r. poz. 1524; dalej: u.o.d.p.w.
[16] Dz.Urz. UE L 119, s. 1; dalej: RODO.

bowiem z ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[17] administratorem danych osobowych gromadzonych w Krajowym Rejestrze Karnym jest Minister Sprawiedliwości.

[17] Tekst jedn. Dz.U. z 2023 r. poz. 1206.

3. W jakim zakresie organy publiczne powinny udostępniać dane z rejestrów publicznych oraz akt rejestrowych przez API i jak zapewnić przy tworzeniu API ochronę danych osobowych?

Dane do ponownego wykorzystywania powinny być udostępniane w zakresie, którego granice wyznacza treść ograniczeń, o których mowa w art. 6 u.o.d.p.w. Należy również zaznaczyć, że zgodnie z art. 10 ust. 1 u.o.d.p.w. podmiot zobowiązany w zakresie ponownego wykorzystywania, jeżeli to możliwe, udostępnia lub przekazuje informacje sektora publicznego, jako otwarte dane zdefiniowane w art. 2 pkt 11 u.o.d.p.w. jako informacje sektora publicznego udostępniane lub przekazywane w postaci elektronicznej kompletne, aktualne, w wersji źródłowej, w otwartym i niezastrzeżonym formacie przeznaczonym do odczytu maszynowego (przykładowo JSON, XML, CSV, RDF) bez konieczności potwierdzania tożsamości przez użytkownika.

Jak stanowi art. 2 pkt 9 u.o.d.p.w., interfejs programistyczny aplikacji (API) to zbiór technicznych funkcji umożliwiających połączenie i wzajemną wymianę danych lub metadanych między programami komputerowymi lub systemami teleinformatycznymi[18]. W rozumieniu informatycznym jest to rozwiązanie stanowiące zestaw reguł algorytmicznych lub protokołów umożliwiających usługom elektronicznym komunikację między sobą w celu przetwarzania danych, realizacji funkcji oczekiwanych przez użytkowników i związanych z nimi funkcjonalności[19]. Oznacza to w praktyce mechanizm (usługę elektroniczną) wymiany danych między systemami teleinformatycznymi bez interfejsu użytkownika (front-endu). Regulacje zawarte w ustawie o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, co do zasady, nie wymagają stosowania takiego rozwiązania. Analizując to zagadnienie od strony pragmatycznej, zaleca się stosowanie API jako mechanizmu, którego działanie powinno być skuteczne, powtarzalne i pozwalające na automatyzację.

Warto dodać, że niektóre dane gromadzone w rejestrach zarządzanych przez Ministerstwo Sprawiedliwości można zaklasyfikować jako dane o wysokiej wartości w rozumieniu art. 2

[18] Pojęcie to pojawia się również m.in. w art. 2 pkt 18 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 321, s. 36, ze zm.).

[19] *What is an API (application programming interface)?*, https://www.ibm.com/topics/api (dostęp: dnia 30 czerwca 2024 r.).

pkt 4 u.o.d.p.w. ze względu na istotne korzyści dla społeczeństwa i gospodarki płynące z ich ponownego wykorzystywania. Zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2023/138 z dnia 21 grudnia 2022 r. ustanawiającym wykaz szczególnych zbiorów danych o wysokiej wartości oraz warunki ich publikacji i ponownego wykorzystywania[20] dane dotyczące przedsiębiorstw i ich własności (nazwa przedsiębiorstwa, status przedsiębiorstwa, data rejestracji, adres siedziby statutowej, forma prawna, numer w rejestrze, państwo członkowskie rejestracji przedsiębiorstwa, rodzaje działalności prowadzonej przez przedsiębiorstwo) są zaliczane do omawianej kategorii. Oznacza to, że przynajmniej w części Krajowy Rejestr Sądowy powinien być uznany za zbiór danych o wysokiej wartości i w takiej sytuacji należy wdrożyć interfejs API pozwalający na wymianę danych w otwartych formatach przeznaczonych do odczytu maszynowego[21], wraz ze stosowną dokumentacją techniczno-organizacyjną. Te zasoby informacyjne powinny być udostępniane na otwartej licencji Creative Commons Uznanie Autorstwa (BY) 4.0.

W okolicznościach zwiększonej interoperacyjności i częściowej automatyzacji czynności w procesach przetwarzania danych w rejestrach zarządzanych przez Ministerstwo Sprawiedliwości potencjalnie istnieje możliwość klasyfikacji części tych zasobów jako danych dynamicznych w rozumieniu art. 2 pkt 3 u.o.d.p.w. ze względu na charakterystyczne dla nich częste aktualizacje, a także zmienność lub szybką dezaktualizację. Po realizacji opisanych przesłanek zgodnie z art. 24 ust. 1 u.o.d.p.w. takie zasoby informacyjne udostępnia się również przez API.

Zapewnienie ochrony danych w systemie teleinformatycznym, którego częścią jest API, polega na realizacji zasad ochrony danych zawartych w art. 5 RODO. Od strony techniczno-organizacyjnej wdrożenie systemu zarządzania bezpieczeństwem informacji przetwarzanych w omawianym rozwiązaniu może dodatkowo implementować wymogi wynikające z rodziny norm ISO 27000. Nie jest to w swojej istocie prawny obowiązek, ale chcąc zabezpieczyć zasoby informatyczne w stopniu wyższym niż minimalny oraz w sposób zorganizowany i sprawdzony, warto rozważyć stosowanie tych standardów. Ma to znaczenie również w kontekście spełnienia w niedalekiej przyszłości wymagań komplementarnego dla obszaru rozważań dotyczących ochrony danych osobowych aktu prawnego – dyrektywy NIS2[22] i jej krajowej implementacji. Zgodnie z art. 5 ust. 3 ustawy z dnia 12 września 2002 r. o normalizacji[23] stosowanie Polskich Norm jest dobrowolne, ale stanowią one zestaw praktyk i wzorców postępowania, które uspraw-

[20] Dz.Urz. UE L 19, s. 43.

[21] Tak stanowi art. 25 ust. 1 pkt 2 i 3 u.o.d.p.w. oraz art. 4b ust. 2 ustawy o Krajowym Rejestrze Sądowym.

[22] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.Urz. UE L 333, s. 80).

[23] Tekst jedn. Dz.U. z 2015 r. poz. 1483.

nia wprowadzenie nie tylko charakterystycznych dla działalności gospodarczej wymagań klienta, ale także powinności, które wynikają wprost z treści przepisów prawa. Innymi słowy standardy takie pozwalają zastosować sprawdzone rynkowo podejście do realizacji określonych działań. Należy zgodzić się z poglądem, że „systemy prawa w obszarze zagadnień technicznych oparte wyłącznie na prawie stanowionym nie są efektywne i powinny być uzupełniane normami technicznymi"[24]. Takie podejście można uznać za ograniczone zastosowanie koncepcji nowego zarządzania publicznego (*New Public Management*)[25].

Przetwarzanie danych osobowych powinno odbywać się w warunkach zapewniających respektowanie takich atrybutów bezpieczeństwa, jak poufność, integralność i dostępność. W RODO uregulowano następujący katalog zasad ochrony tych zasobów informacyjnych:

1) zgodność z prawem, rzetelność i przejrzystość – przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a);
2) ograniczenie celu – zbieranie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; jednak dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami (art. 5 ust. 1 lit. b);
3) minimalizacja danych – adekwatność, stosowność oraz ograniczenie do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c);
4) prawidłowość – prawidłowość i w razie potrzeby uaktualnianie; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (art. 5 ust. 1 lit. d);
5) ograniczenie przechowywania – 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, a zarazem 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, z zastrzeżeniem że wdrożone zostaną odpowiednie do okoliczności środki techniczne i organizacyjne (art. 5 ust. 1 lit. e);
6) integralność i poufność – 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 (art. 5 ust. 1 lit. f);

[24] B. Fischer, *Prawne aspekty norm technicznych. Normalizacja jako wsparcie legislacji administracyjnej*, Warszawa 2017, s. 260.

[25] L. Rajca, *Koncepcja New Public Management a reformy samorządu terytorialnego wybranych państw Europy Zachodniej*, „Studia Regionalne i Lokalne" 2009, nr 2(36), s. 72.

7) rozliczalność – możność wykazywania zgodności podejmowanych działań w zakresie ochrony z wymaganiami prawnymi, a w szczególności wymienionymi wcześniej zasadami (art. 5 ust. 2).

Realizacja wymienionych zasad wymaga do administratora danych, zgodnie z art. 4 pkt 7 RODO ustalającego cele i sposoby przetwarzania, zastosowania odpowiednich do zagrożeń chronionych zasobów środków organizacyjnych (wewnętrzne polityki i procedury, zapisy, szkolenia, komunikaty o zagrożeniach) i technicznych (mechanizmy autoryzacji i uwierzytelniania użytkowników, szyfrowanie, kopie zapasowe, przeciwdziałanie złośliwemu oprogramowaniu, rejestracja zdarzeń, inwentaryzacja urządzeń i nośników).

Obowiązki administratora danych możemy podzielić na te, które dotyczą:

1) realizacji praw podmiotów danych:
   a) realizacja obowiązku informacyjnego,
   b) respektowanie prawa do bycia zapomnianym, w tym usunięcia danych,
   c) uwzględnienie sprzeciwu wobec przetwarzania danych;
   d) umożliwienie przenoszenia danych,
   e) akceptacja cofnięcia zgody na przetwarzanie danych,
   f) zawiadomienie o wystąpieniu naruszenia ochrony danych;
2) zapewnienia bezpieczeństwa przetwarzanych danych:
   a) prowadzenie dokumentacji związanej z przetwarzaniem danych, w tym:
      – wykonywanie uprzedniej oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem tego procesu,
      – utrzymywanie rejestru czynności przetwarzania danych osobowych,
      – wdrażanie polityki ochrony danych;
   b) udzielenie upoważnień dla osób przetwarzających dane w imieniu administratora w ramach organizacji,
   c) zawarcie umowy powierzenia, jeśli proces przetwarzania technicznie realizowany jest przez podmiot zewnętrzny,
   d) wdrożenie adekwatnych do stopnia ryzyka przetwarzania środków techniczno-organizacyjnych,
   e) budowanie świadomości o zagrożeniach, ich konsekwencjach i sposobach przeciwdziałania im, a także szkolenie osób, które uczestniczą w procesie przetwarzania danych;
3) wykonywania powinności wobec organu nadzorczego, czyli Prezesa Urzędu Ochrony Danych Osobowych:
   a) zgłaszanie naruszeń ochrony danych osobowych,
   b) informowanie o powołaniu inspektora ochrony danych,
   c) w czasie kontroli stworzenie organowi nadzorczemu warunków umożliwiających jej skuteczne przeprowadzenie.

Obecnie – w odróżnieniu od stanu prawnego wynikającego z obowiązywania ustawy o ochronie danych osobowych z 1997 r.[26] – regulacje dotyczące ochrony danych osobowych nie określają zamkniętego katalogu środków techniczno-organizacyjnych (zabezpieczeń) niezbędnych do zastosowania, aby zapewnić bezpieczeństwo przetwarzanych zasobów. Zgodnie z art. 24 RODO administrator danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z prawem i aby móc to wykazać (co stanowi realizację zasady rozliczalności wyrażonej w art. 5 ust. 2 RODO). Przykładowe rozwiązania z tego obszaru wskazano w art. 32 ust. 1 RODO:

1) pseudonimizacja i szyfrowanie danych osobowych;
2) utrzymywanie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
3) utrzymywanie zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W kontekście rejestrów zarządzanych przez Ministerstwo Sprawiedliwości warto rozważyć stworzenie kodeksu postępowania, o którym mowa w art. 32 ust. 3 RODO. Instrument ten ujednolici i uporządkuje podejście do stosowania środków techniczno-organizacyjnych w celu zabezpieczenia danych gromadzonych w poszczególnych rejestrach publicznych. Procedura ustanawiania kodeksów postępowania została wyrażona w art. 40 RODO. Warto zaznaczyć, że organ opiniodawczo-doradczy, jakim jest Europejska Rada Ochrony Danych, działając na podstawie art. 70 ust. 1 lit. e RODO, wydała wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679[27]. Zgodnie z tym dokumentem można zidentyfikować następujące korzyści ze stosowania takiego instrumentu:

1) ustanowienie zbioru reguł, które przyczyniają się do odpowiedniego stosowania RODO w sposób praktyczny, przejrzysty i ekonomiczny, a przy tym uwzględniający specyfikę danego sektora lub charakterystycznych dla niego czynności przetwarzania;
2) wspomagają administratora i podmiot przetwarzający w przestrzeganiu RODO poprzez uporządkowanie i doszczegółowienie wymagań w takich obszarach, jak rzetelne i przejrzyste przetwarzanie danych, prawnie uzasadnione interesy, środki bezpieczeństwa

[26] Mowa tu o nieobowiązującej już ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133 poz. 883).

[27] Zob. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pl.pdf (dostęp: dnia 28 września 2024 r.).

i ochrony danych już w fazie projektowania oraz domyślna ochrona danych, a także obowiązki administratora;

3) stanowią przejaw samoregulacji przez administratorów dodatkowo zatwierdzanej przez organ nadzorczy, co zwiększa prawdopodobieństwo właściwego stosowania ogólnych wymagań z RODO;
4) respektują autonomię i prawo do samokontroli przez administratorów oraz podmioty przetwarzające w procesie formułowania i uzgadniania reguł najlepszych praktyk w przypadku ich danych sektorów;
5) zapewniają niezbędne zaufanie i gwarantują pewność prawa poprzez dostarczenie praktycznych rozwiązań problemów zidentyfikowanych przez poszczególne sektory w odniesieniu do wspólnych czynności przetwarzania;
6) budują zaufanie osób, których dane dotyczą, poprzez doprecyzowanie w kontekście stosowania w danym sektorze generalnych i abstrakcyjnych norm wynikających z RODO;
7) stanowią wsparcie w obszarze ustanowienia jednolitych i przejrzystych reguł międzynarodowego przekazywania danych;
8) stosowanie zatwierdzonego kodeksu postępowania jest uwzględniane przez organy nadzorcze przy ocenie konkretnych cech przetwarzania danych, takich jak respektowanie wymagań bezpieczeństwa w stosunku do poszczególnych czynności przetwarzania, przy ocenie skutków operacji przetwarzania w ramach oceny skutków dla ochrony danych lub przy nakładaniu administracyjnej kary pieniężnej.

Do celów stosowania omawianych kodeksów postępowania należą następujące kwestie:

1) doprecyzowanie stosowania RODO w stosunku do konkretnych okoliczności przetwarzania danych;
2) zapewnienie wystarczających zabezpieczeń przetwarzanych zasobów;
3) zapewnienie mechanizmów umożliwiających skuteczny nadzór.

Kolejnym istotnym elementem porządkowania podejścia do ochrony danych w ramach procesów zarządzania poszczególnymi rejestrami publicznymi jest ustanowienie spójnych, kompleksowych i skutecznych polityk ochrony danych. Są to plany lub sposoby działania przyjęte w celu zapewnienia bezpieczeństwa systemów i ochrony danych w organizacji[28]. Omawiany dokument powinien być dostosowany do konkretnych warunków przetwarzania danych osobowych u określonego administratora danych[29]. Zgodnie z normą ISO 27001[30] najwyższe kierownictwo powinno ustanowić politykę bezpieczeństwa informacji, która:

---

[28] A. Białas, *Polityka bezpieczeństwa w rozproszonych systemach komputerowych* [w:] A. Grzywak (red.), *Internet w społeczeństwie informacyjnym*, Dąbrowa Górnicza 2003, s. 207.

[29] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 5 października 2005 r., II SA/Wa 734/05, LEX nr 217395.

[30] PN-EN ISO/IEC 27001:2023-08 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

1) odpowiada celowi istnienia organizacji,
2) zawiera cele bezpieczeństwa informacji lub tworzy ramy do ustanowienia celów bezpieczeństwa informacji,
3) zawiera zobowiązanie do spełnienia mających zastosowanie wymagań dotyczących bezpieczeństwa informacji, oraz
4) zawiera zobowiązanie do ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji.

Polityka bezpieczeństwa informacji powinna być:

1) dostępna jako udokumentowana informacja,
2) zakomunikowana w organizacji, oraz
3) dostępna dla stron zainteresowanych, jeśli jest to właściwe.

Norma ISO 27002[31] podaje zaś następujące wytyczne dotyczące wdrożenia polityk bezpieczeństwa jako zabezpieczenia organizacyjnego:

1) cel zabezpieczenia: wskazanie kierunku zarządzania i wsparcia dla bezpieczeństwa informacji w zgodzie z wymaganiami biznesowymi i odpowiednimi przepisami powszechnie obowiązującymi i innymi regulacjami (wytyczne i wsparcie dla kierownictwa);
2) zabezpieczenie: dokument polityki bezpieczeństwa informacji powinien być zatwierdzony przez kierownictwo, opublikowany, zakomunikowany wszystkim pracownikom i innym podmiotom współpracującym z organizacją;
3) wskazówki dotyczące wdrożenia: na najwyższym poziomie organizacje powinny zdefiniować „politykę bezpieczeństwa informacji", która określa podejście organizacji do zarządzania bezpieczeństwem informacji prowadzące do realizacji jej celów. Dokument ten powinien zostać zatwierdzony przez kierownictwo;
4) dodatkowe informacje: potrzeby istnienia wewnętrznych polityk szczegółowych powinny wynikać ze specyfiki procesów funkcjonujących w konkretnej organizacji. Te dodatkowe instrumenty zarządcze mogą być szczególne użyteczne w przypadku dużych i złożonych organizacji, gdzie definiowanie poziomów zabezpieczeń i ich implementacji jest przypisane do osobnych jednostek organizacyjnych, a także w sytuacjach, kiedy polityki wprowadzane są w zespołach o zróżnicowanych kompetencjach i funkcjach w organizacji. Dokument polityki może być pojedynczym dokumentem lub zespołem powiązanych ze sobą dokumentów.

Polityka bezpieczeństwa obejmuje wymagania wynikające:

1) ze strategii biznesowej;
2) z aktów prawnych i innych regulacji, a także umów;

[31] PN-EN ISO/IEC 27002:2023-01 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji.

3) z bieżącego i przewidywanego stanu zagrożeń dla bezpieczeństwa informacji w środowisku organizacji.

Rozpatrywany dokument uwzględnia również zakres i granice Systemu Zarządzania Bezpieczeństwem Informacji w organizacji. Polityka bezpieczeństwa informacji zawiera deklaracje dotyczące:

1) definicji bezpieczeństwa informacji, celów i zasad obejmujących wszystkie działania związane z bezpieczeństwem informacji;
2) przypisania ogólnych i szczegółowych obowiązków w zakresie zarządzania bezpieczeństwem informacji do wcześniej zdefiniowanych ról;
3) procedur wprowadzania odstępstw i wyjątków.

Na niższym poziomie polityka bezpieczeństwa informacji powinna być wspierana przez polityki tematyczne, wymagające wdrożenia określonych rodzajów zabezpieczeń informacji:

1) kontrola dostępu;
2) klasyfikacja informacji (i ich obsługa);
3) bezpieczeństwo fizyczne i środowiskowe;
4) tematy dotyczące użytkownika końcowego, takie jak:
   a) dopuszczalne wykorzystanie aktywów,
   b) reguła czystego biurka i ekranu,
   c) przekazywanie informacji,
   d) urządzenia mobilne i telepraca,
   e) ograniczenia dotyczące instalacji oprogramowania i jego wykorzystywania;
5) tworzenia kopii zapasowych;
6) przetwarzanie informacji;
7) ochrona przed złośliwym oprogramowaniem;
8) zarządzanie podatnościami technicznymi;
9) zabezpieczenia kryptograficzne;
10) bezpieczeństwo komunikacji;
11) prywatność i ochrona danych osobowych;
12) relacje z dostawcami.

Dokumenty te zazwyczaj są tak skonstruowane, aby zaspokajać potrzeby określonych grup docelowych w ramach organizacji lub kompleksowo regulować niektóre tematy. Polityka powinna być zakomunikowana pracownikom i zainteresowanym stronom zewnętrznym w odpowiedniej, przystępnej i zrozumiałej formie zgodnej z programem zwiększania świadomości, edukacji i treningu dotyczącego bezpieczeństwa informacji. Jeśli dokument polityki bezpieczeństwa jest dystrybuowany poza organizację, to dostęp powinno się ograniczyć do znajdujących się w nim poufnych informacji organizacji.

Przykładowa struktura dokumentu polityki opracowana na podstawie normy ISO 27003[32]:

1) streszczenie – określenie ogólnej charakterystyki tego dokumentu;
2) wstęp – zwięzłe przedstawienie tematyki polityk;
3) zakres – opisuje, jakie części organizacji są objęte polityką. Jeśli jest to zasadne, to wskazuje się wspierane przez ten dokument inne polityki;
4) cele – opisują istotne intencje związane ze sformułowaniem tej polityki;
5) zasady – opisują sposoby działania i podejmowania decyzji służących osiąganiu celów. W niektórych sytuacjach przydatne może być zidentyfikowanie kluczowych procesów związanych z tematem polityki i związanych z ich funkcjonowaniem reguł;
6) obowiązki – ta część opisuje, kto jest odpowiedzialny za działania mające doprowadzić do wypełnienia celów i realizacji wymagań zawartych w polityce. W niektórych przypadkach ten element dokumentacji może obejmować opis struktury organizacyjnej, jak również zawierać wykaz powinności osób pełniących określone funkcje;
7) kluczowe wyniki – jest to wykaz rezultatów biznesowych, które zostaną osiągnięte, jeśli cele polityki będą realizowane;
8) powiązane polityki – wykaz innych polityk zawierających rekomendacje dotyczące konkretnych tematów istotnych dla osiągnięcia celów omawianego dokumentu.

Dla ciągłego utrzymywania bezpieczeństwa przetwarzanych zasobów informacyjnych przez cały ich cykl życia fundamentalne znaczenie ma uporządkowanie procesu zarządzania ryzykiem. Zgodnie z motywem 75 RODO ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych. Dodatkowo motyw 76 RODO precyzuje, że prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Powszechnie uznanym standardem prowadzenia procesu zarządzania ryzykiem w obszarze bezpieczeństwa informacji jest norma ISO 27005[33]. W ramach działalności edukacyjnej Urzędu Ochrony Danych wskazano ten standard jako referencyjny dla obsługi ryzyka w procesach przetwarzania danych osobowych[34].

Zarządzanie ryzykiem jest jednym z kilku elementów procesu zarządzania bezpieczeństwem systemów teleinformatycznych, których celem jest udzielenie odpowiedzi na następujące pytania:

---

[32] ISO/IEC 27003:2017 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wytyczne (*Information technology – Security techniques – Information security management systems – Guidance*).

[33] PN-ISO/IEC 27005:2018, Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

[34] *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku*, cz. 1, https://archiwum.uodo.gov.pl/pl/file/706; *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku*, cz. 2, https://archiwum.uodo.gov.pl/pl/file/707 (dostęp: dnia 30 czerwca 2024 r.).

1) co złego może się wydarzyć,
2) jakie jest prawdopodobieństwo, że wydarzy się coś złego,
3) jakie skutki dla systemu informatycznego i organizacji będą miały te wydarzenia,
4) jak i ile możemy zmniejszyć straty.

Proces zarządzania ryzykiem bezpieczeństwa informacji składa się z następujących faz zgodnych z podejściem opartym na cyklu Deminga (ang. *Plan – Do – Check - Act*), zakładającym stosowanie koncepcji ciągłego doskonalenia zarządzanych procesów:

1) planowanie:
   a) ustanowienie kontekstu,
   b) szacowanie ryzyka,
   c) opracowanie planu postępowania z ryzykiem,
   d) akceptowanie ryzyka;
2) wykonywanie – wdrożenie planu postępowania z ryzykiem;
3) sprawdzanie – ciągłe monitorowanie i przegląd ryzyka;
4) działanie – utrzymywanie i doskonalenie procesu zarządzania ryzykiem w bezpieczeństwie informacji.

Podstawowy dla analizowanej koncepcji etap szacowania ryzyka powinien obejmować następujące czynności:

1) identyfikację zagrożeń i ich źródeł;
2) identyfikację istniejących i planowanych zabezpieczeń;
3) identyfikację luk w zabezpieczeniach, które mogą być wykorzystane przez zagrożenia, aby wyrządzić szkody organizacji i jej zasobom;
4) identyfikację konsekwencji utraty poufności, integralności, dostępności, niezaprzeczalności i innych atrybutów charakterystycznych dla przetwarzanych zasobów informacyjnych;
5) ocenę wpływu biznesowego, który może być rezultatem przewidywanych lub faktycznych incydentów związanych z bezpieczeństwem informacji;
6) ocenę prawdopodobieństwa określonych scenariuszy incydentów (zawierają one opis zagrożenia wykorzystującego określoną podatność – lukę lub zestaw słabych punktów, w ramach incydentu dotyczącego bezpieczeństwa informacji);
7) ocenę (oszacowanie) poziomu ryzyka;
8) porównanie poziomów ryzyka z kryteriami oceny ryzyka i kryteriami akceptacji ryzyka.

Wynik analizy ryzyka ma szczególne znaczenie przy sporządzaniu oceny skutków dla ochrony danych przewidzianej w art. 35 RODO. Powinna być ona sporządzona przed rozpoczęciem przetwarzania danych lub po wprowadzeniu istotnych zmian w ramach istniejących czynności przetwarzania danych, przykładowo poprzez zastosowanie nowej technologii (m.in. zastosowanie rozwiązań sztucznej inteligencji). Obowiązek ten materializuje się

w sytuacji wystąpienia dużego prawdopodobieństwa wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

De lege ferenda i w odniesieniu do praktyki administracyjno-zarządczej należy rozważyć, czy nie byłoby zasadne rozszerzenie koncepcji Portalu Rejestrów Sądowych na wszystkie rejestry publiczne zarządzane przez Ministerstwo Sprawiedliwości[35]. W szczególności uwagi te dotyczą następujących kwestii.

1. Struktury danych o podobnych cechach znaczników i metadanych (czyli ustrukturyzowanych informacjach opisujących, tłumaczących, lokalizujących i ułatwiających odnalezienie, wykorzystanie innych informacji lub zarządzanie nimi) – podstawową ideą jest w analizowanym przypadku to, aby tworzyły one strukturę drzewa reprezentującą różne typy danych, kategorie i podkategorie rejestrów zarządzanych przez Ministerstwo Sprawiedliwości. Zaletą tego rozwiązania jest to, że w razie przyszłej reorganizacji struktury rejestrów publicznych łatwiejsze będzie umiejscowienie i zdefiniowanie nowych/podlegających zmianie elementów.
2. Ujednolicony *front-end*, czyli struktura interfejsu użytkownika, identyfikacji wizualnej (kolorystyka, obrazki – logo, rozmieszczenie treści na stronie WWW).
3. Zaproponowanie referencyjnej (podstawowej) struktury formularzy realizujących podobne cele w każdym z rejestrów – np. wyszukiwanie, składanie wniosków o aktualizację danych, dostępu do dokumentów związanych z konkretnym rekordem rejestru (wpisem).
4. Zarządzanie kontrolą dostępu do poszczególnych rejestrów w sposób możliwie jednorodny (pod względem ról użytkowników, przysługujących im uprawnień i powiązanych polityk).

Podstawowym celem sformułowanych propozycji jest ograniczenie nieuzasadnionej względami prawnymi i praktycznymi różnorodności poszczególnych elementów systemów teleinformatycznych i w ten sposób obniżenie kosztu ich ewentualnej modyfikacji. Należy zaznaczyć, że nie chodzi tu o całkowitą integrację wszystkich rejestrów, a o docelowe ustalenie wspólnych techniczno-organizacyjnych reguł ich prowadzenia. Poniższe uwagi zostały poczynione ze względu na fakt, że realizacja prawa do ponownego wykorzystywania jest niejako jednym z pięter struktury zarządzania rejestrami pozostającymi w gestii Ministerstwa Sprawiedliwości. Zaprezentowana warstwowa koncepcja instytucji prawnych, procedur, rozwiązań organizacyjnych i systemów teleinformatycznych jest rozwinięciem idei Architektury Informacyjnej Państwa[36]. Implementuje ona założenia architektury korporacyjnej

[35] Rozważyć tu można swoisty rodzaj współpracy międzyresortowej oraz wykorzystanie doświadczeń i dobrych praktyk uzyskanych w ramach realizacji projektu „System Rejestrów Państwowych".

[36] Zob. https://www.gov.pl/web/cyfryzacja/architektura-informacyjna-panstwa (dostęp: dnia 30 czerwca 2024 r.).

zakładającej rozumienie organizacji jako zbioru elementów z perspektywy biznesowej i technicznej połączonych wzajemnymi relacjami horyzontalnie i wertykalnie, których realizacja ma prowadzić do realizacji celów tej struktury[37]. Zastosowanie takiego podejścia powinno ułatwiać zaprojektowanie, zorganizowanie i bieżące skuteczne zarządzanie heterogenicznymi obszarami funkcjonowania organizacji – również takiej jak administracja publiczna i jej organy[38].

Należy rozważyć również dalszą integrację i zwiększenie poziomu interoperacyjności zarządzanych przez Ministerstwo Sprawiedliwości zasobów informacyjnych podlegających udostępnieniu w ramach realizacji z portalem danych w rozumieniu art. 2 pkt 13 u.o.d.p.w. (dane.gov.pl). Najrozsądniejszym podejściem wydaje się traktowanie go jako front-endu dla istniejących już rozwiązań, co pozwoli zredukować koszty prowadzenia samodzielnie zarządzanego interfejsu użytkownika, a także istotnie zmniejszy nakłady na zabezpieczanie takich elementów systemów teleinformatycznych.

[37] V. Boucharas, M. van Steenbergen, S. Jansen, S. Brinkkemper, *The Contribution of Enterprise Architecture to the Achievement of Organizational Goals: A Review of the Evidence* [w:] E. Proper, M. Lankhorst, M. Schönherr, J. Barjis, S. Overbeek, *Trends in Enterprise Architecture Research*, 5th Workshop, TEAR 2010, Berlin Heidelberg 2010, s. 1–2.

[38] B. Szafrański, *Architektura korporacyjna – problemy nie tylko pojęciowe*, „Roczniki Kolegium Analiz Ekonomicznych" 2015, nr 38, s. 273.

4. W jakim zakresie organy publiczne powinny udostępniać dane z rejestrów publicznym i akt rejestrowych na wniosek, z uwzględnieniem ochrony danych osobowych?

Decyzja co do zakresu udostępniania danych na wniosek determinuje wspomniana wcześniej treść art. 6 u.o.d.p.w. Nie można zapominać również, że pomimo wyrażonej w art. 14 ust. 2 u.o.d.p.w. zasady bezwarunkowości udostępniania informacji publicznej do ponownego wykorzystywania istnieje możliwość ustalenia warunków na podstawie art. 15 u.o.d.p.w. Wynika ona z faktu, że rejestry publiczne można traktować jako bazy danych w rozumieniu art. 2 ust. 1 pkt 1 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych[39]. Są to przecież w istocie zbiory danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagające istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji ich zawartości. Na potwierdzenie tego stanowiska można wskazać, że w ramach treści informacyjnych dostępnych na stronie internetowej polskiego punktu kontaktowego (Punktu Informacji dla Przedsiębiorcy) utworzonego na podstawie ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy[40] rejestry publiczne prowadzone przez instytucje państwowe zapewniają dostęp do składających się na nie baz danych[41]. Dodatkowo wprost w art. 4 ust. 1 ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich określono, że Rejestr Sprawców Przestępstw na Tle Seksualnym składa się z baz danych.

Na podstawie art. 15 ust. 1 u.o.d.p.w. można ustanowić warunki ponownego wykorzystywania informacji sektora publicznego dotyczące następujących zagadnień:

1) obowiązku poinformowania o źródle, czasie wytworzenia i pozyskania informacji sektora publicznego od podmiotu zobowiązanego lub

---

[39] Tekst jedn. Dz.U. z 2021 r. poz. 386 ze zm.

[40] Tekst jedn. Dz.U. z 2022 r. poz. 541.

[41] *Rejestry publiczne – jakie bazy danych są dostępne dla firm*, https://www.biznes.gov.pl/pl/portal/00152 (dostęp: dnia 30 czerwca 2024 r.).

2) obowiązku poinformowania o przetworzeniu informacji sektora publicznego ponownie wykorzystywanych, lub
3) zakresu odpowiedzialności podmiotu zobowiązanego za udostępniane lub przekazywane w celu ponownego wykorzystywania informacje sektora publicznego, w szczególności za dostępność, poprawność, aktualność, kompletność lub jakość udostępnianych lub przekazywanych informacji, lub
4) informacji sektora publicznego stanowiących lub zawierających dane osobowe.

Zgodnie z art. 4 pkt 1 RODO dane osobowe oznaczają „wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej". W ramach decyzji administracyjnej w sprawie dotyczącej udostępnienia danych z Ksiąg Wieczystych (w postaci ich numerów) Urząd Ochrony Danych Osobowych zwrócił uwagę na możliwość wystąpienia szeregu negatywnych konsekwencji dla osoby fizycznej w związku z udostępnieniem publicznie numeru PESEL, który jest bez wątpliwości jej numerem identyfikacyjnym w rozumieniu RODO. Ponadto w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 5 maja 2021 r., sygn. akt. II Sa/Wa 2222/20[42], wskazany sąd potwierdził stanowisko Urzędu Ochrony Danych Osobowych, że już same numery ksiąg wieczystych są danymi osobowymi ze względu na możliwość ustalenia na ich podstawie przede wszystkim informacji o tożsamości właściciela nieruchomości.

Zaznaczyć również należy, że co do zasady publiczne udostępnianie danych z rejestrów publicznych, w sytuacji gdy zrealizowana jest przesłanka legalizująca wymieniona w art. 6 ust. 1 lit. e RODO, jest zgodne z prawem. Przykładowo, w odniesieniu do Krajowego Rejestru Sądowego w art. 8 ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym wprowadzono zasadę jawności formalnej, która spełnia wspomniane wymagania RODO i jest zgodna z zasadą legalizmu wyrażoną w art. 5 ust. 1 lit. a RODO[43].

Przesłanki legalizujące przetwarzanie tzw. danych zwykłych reguluje art. 6 RODO. Należy jednak pamiętać o tym, że w niektórych rejestrach zarządzanych przez Ministerstwo Sprawiedliwości odnajdziemy także szczególne kategorie danych osobowych (tzw. dane wrażliwe – art. 9 RODO), a także dane dotyczące wyroków skazujących i czynów zabronionych (art. 10 RODO).

[42] LEX nr 3209095.

[43] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 30 stycznia 2019 r., sygn. ZSPU.440.574.2018, https://uodo.gov.pl/decyzje/ZSPU.440.574.2018 (dostęp: dnia 29 września 2024 r.).

5. Czy możliwe jest ustalenie w prawie krajowym dodatkowych wymogów dotyczących wniosku, np. wymogu złożenia go przez system teleinformatyczny w postaci elektronicznej?

Zgodnie z art. 39 ust. 4 u.o.d.p.w. wniosek o ponowne wykorzystywanie wnosi się w postaci papierowej albo elektronicznej. Biorąc pod uwagę, że adresatem tej konkretnej normy szczegółowej jest wnioskodawca, wydaje się, iż ograniczenie jego praw wyboru postaci wniosku nie byłoby przy istniejącym stanie prawnym możliwe. Należy jednak zaznaczyć, że w art. 4 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego[44] – której implementacja w polskim porządku prawnym jest w tym opracowaniu analizowana – nie przesądza się o postaci wniosku, a nawet niejako faworyzuje się tę elektroniczną („w miarę możliwości i stosownie do przypadku przy wykorzystaniu środków elektronicznych"). Biorąc pod uwagę materię ponownego wykorzystywania, która jest mocno związana z przetwarzaniem danych w postaci elektronicznej, ograniczenie wniosku tylko do niej byłoby zasadne, ale wymaga przy tym dokonania zmian legislacyjnych rangi ustawowej[45].

[44] Dz.Urz. UE L 172, s. 56.

[45] Warto tutaj dodać, że dla przykładu obecnie rekrutacja na studia na większości uczelni wyższych w Polsce odbywa się wyłącznie za pośrednictwem elektronicznego systemu teleinformatycznego „Internetowa Rejestracja Kandydatów".

6. Czy fakt jednoczesnej dostępności danych w publicznym rejestrze uzasadnia w świetle przepisów Unii Europejskiej odmowę uwzględnienia wniosku o ich udostępnienie?

Zgodnie z art. 5 u.o.d.p.w. każdemu przysługuje prawo do ponownego wykorzystywania informacji sektora publicznego i mogą być one udostępniane na następujące sposoby:

1) w Biuletynie Informacji Publicznej podmiotu zobowiązanego lub w portalu danych, lub w innym systemie teleinformatycznym podmiotu zobowiązanego;
2) przekazywane na wniosek o ponowne wykorzystywanie.

W tej kwestii istnieje możliwość poinformowania wnioskodawcy, że te dane są dostępne w publicznym rejestrze dostępnym za pośrednictwem API lub prostej wyszukiwarki z interfejsem graficznym obsługiwanej z poziomu przeglądarki. Rozwiązania takie stanowią inny system teleinformatyczny podmiotu zobowiązanego zgodnie z art. 5 pkt 1 u.o.d.p.w. Oznacza to zatem, że cel regulacji w postaci udostępnienia danych do ponownego wykorzystywania został w praktyce zrealizowany. W takiej sytuacji zamiast odmowy udostępnienia informujemy wnioskodawcę o sposobie dostępu w ramach czynności materialno-technicznej[46].

[46] Jak wskazano w literaturze: „zauważyć również trzeba, że negatywne rozstrzygnięcie którejkolwiek ze wskazanych okoliczności powoduje konieczność stosownego poinformowania wnioskodawcy w drodze czynności materialno-technicznej" (B. Fischer i in., *Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Warszawa 2022, art. 39).

7. Krótka charakterystyka toczących się lub planowanych prac legislacyjnych związanych z tematem badawczym

Analizowana jest konieczność uzupełnienia przepisów ustaw rejestrowych pozostających we właściwości Ministra Sprawiedliwości pod kątem spójności z ustawą z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego oraz przepisami prawa Unii Europejskiej.

Bibliografia

Białas A., *Polityka bezpieczeństwa w rozproszonych systemach komputerowych* [w:] A. Grzywak (red.), *Internet w społeczeństwie informacyjnym*, Dąbrowa Górnicza 2003.

Boucharas V., Steenbergen M., Jansen S., Brinkkemper S., *The Contribution of Enterprise Architecture to the Achievement of Organizational Goals: A Review of the Evidence* [w:] E. Proper, M. Lankhorst, M. Schönherr, J. Barjis, S. Overbeek, *Trends in Enterprise Architecture Research*, 5th Workshop, TEAR 2010, Berlin Heidelberg 2010.

Fischer B., *Prawne aspekty norm technicznych. Normalizacja jako wsparcie legislacji administracyjnej*, Warszawa 2017.

Fischer B. i in., *Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Warszawa 2022.

Rajca L., *Koncepcja New Public Management a reformy samorządu terytorialnego wybranych państw Europy Zachodniej*, „Studia Regionalne i Lokalne" 2009, nr 2(36).

Szafrański B., *Architektura korporacyjna – problemy nie tylko pojęciowe*, „Roczniki Kolegium Analiz Ekonomicznych" 2015, nr 38.