Bezpieczeństwo informacji w świecie na przykładzie Kasy Rolniczego Ubezpieczenia Społecznego ze szczególnym uwzględnieniem ochrony danych osobowych

Katarzyna Banach, Martyna Lechowicz, Magdalena Szewczyk

Abstrakt

Społeczeństwo informacyjne, w którym informacja posiada coraz większe znaczenie, naraża swoich obywateli na szczególną kategorię cyberzagrożeń, jaką jest naruszenie bezpieczeństwa i poufności informacji oraz nielegalnego wykorzystywania danych osobowych, co w efekcie często prowadzi do kradzieży tożsamości. Dlatego też w celu zapewnienia bezpieczeństwa informacji, a w szczególności ochrony danych osobowych, powstały prawa oraz reguły pozwalające określić sposób zarządzania, przetwarzania, ochrony i dystrybucji tych informacji. Od 28 maja 2018 roku odpowiedzialność za naruszenie bezpieczeństwa danych ponoszą zarówno administrator, jak i podmiot przetwarzający dane. Formy pozyskania i wykorzystania informacji mają swoje odzwierciedlenie w obowiązujących przepisach. W związku z tym podmioty publiczne opracowują Polityki bezpieczeństwa – dokumenty, które zawierają procedury i wewnętrzne zasady postępowania. Ich celem jest wprowadzenie standardów zabezpieczeń informacji oraz zaangażowanie pracowników w aktywne dbanie o bezpieczeństwo danych.

Głównym celem opracowania jest przedstawienie sposobu zapewnienia bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych na przykładzie Kasy Rolniczego Ubezpieczenia Społecznego.

Słowa kluczowe: bezpieczeństwo informacji, dane osobowe, informacja, KRUS, ochrona danych osobowych, polityka bezpieczeństwa.

Katarzyna Banach, słuchaczka studiów podyplomowych „Rolnicze Ubezpieczenia Społeczne – funkcjonowanie, administracja i aspekty prawne" na Uniwersytecie Kaliskim im. Prezydenta Stanisława Wojciechowskiego w Kaliszu, główny specjalista, Zespół Obsługi Rady Ubezpieczenia Społecznego Rolników, Centrala, Kasa Rolniczego Ubezpieczenia Społecznego; **Martyna Lechowicz**, słuchaczka studiów podyplomowych „Rolnicze Ubezpieczenia Społeczne – funkcjonowanie, administracja i aspekty prawne" na Uniwersytecie Kaliskim im. Prezydenta Stanisława Wojciechowskiego w Kaliszu, główny specjalista, Biuro Zarządzania Kryzysowego, Spraw Obronnych i Bezpieczeństwa Informacji, Centrala, Kasa Rolniczego Ubezpieczenia Społecznego; **Magdalena Szewczyk**, słuchaczka studiów podyplomowych „Rolnicze Ubezpieczenia Społeczne – funkcjonowanie, administracja i aspekty prawne" na Uniwersytecie Kaliskim im. Prezydenta Stanisława Wojciechowskiego w Kaliszu, główny specjalista, Biuro Prezesa, Centrala, Kasa Rolniczego Ubezpieczenia Społecznego.

Wstęp

Powstanie społeczeństwa informacyjnego wiąże się z „dynamicznym rozwojem szeroko rozumianych technologii informacyjnych, umożliwiających zdobywanie, przetwarzanie, udostępnianie i przechowywanie informacji”[1]. Tym samym podstawowym towarem jest produkt cyfrowy, czyli informacja (dokumenty, pieniądze, utwory muzyczne, oprogramowanie). To jeden z najistotniejszych czynników, które kształtują ludzkie społeczności. Wynalezienie nowych środków przekazu informacji stało się natomiast czynnikiem prowadzącym do znacznych przemian cywilizacyjnych. Upowszechnienie komputerów osobistych i rozwój dostępu do Internetu doprowadziły do uzyskania przez nie wpływu na kolejne sfery życia społecznego. To z kolei wpłynęło na szerszy rozwój technologii cyfrowych. Informacja bardzo zyskała na znaczeniu – w pewien sposób stała się elementem strategicznym, gdyż nastąpił wyraźny wzrost jej znaczenia nie tylko dla obywateli, lecz także dla instytucji publicznych i prywatnych. Ponieważ informacja pełni wiele istotnych funkcji – m.in. decyzyjną, kulturotwórczą oraz wspierającą rozwój wiedzy – powinna być odpowiednio zarządzana. Wprowadzenie Polityki bezpieczeństwa, której celem jest opracowanie wewnętrznych procedur i regulacji określających zasady postępowania, umożliwia wdrożenie standardów ochrony informacji i angażuje pracowników w ich aktywną ochronę.

Rewolucja w komunikacji, biorąc pod uwagę szybkość i zasięg wymiany informacji, dokonała się dzięki Internetowi, który zapewnił szybki i łatwy dostęp do danych – bez ograniczeń czasowych i geograficznych. Niestety Internet przyniósł ze sobą także nowe ryzyka i nowe zagrożenia. Związane są one z bezpieczeństwem informacji, systemów teleinformatycznych oraz prywatnością. Bezpieczeństwo informacji wymusza, aby zasoby informatyczne były tak zabezpieczone, aby informacje można było gromadzić, przetwarzać, przechowywać i przesyłać w sposób bezpieczny, bez narażania ich na jakiekolwiek zagrożenia.

1. T.R. Aleksandrowicz, *Analityk informacji w administracji rządowej* [w:] *Analiza informacji w zarządzaniu bezpieczeństwem. Zarządzaniem bezpieczeństwem*, (red.) K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa, Wyd. Difin SA, 2013, s. 11.

Sposoby zabezpieczenia informacji, czyli bezpieczeństwo informacji

Podstawowym zadaniem państwa jest zapewnienie bezpieczeństwa i wolności obywateli. Zapisy Konstytucji Rzeczypospolitej Polskiej z 1997 roku[2] wskazują, że bezpieczeństwo odnosi się do wielu kontekstów: publicznego, państwa, obywatela, wewnętrznego i zewnętrznego, ekologicznego. Art. 5 Konstytucji RP stanowi, iż „państwo strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując zasadą zrównoważonego rozwoju"[3]. Jak widać, zagwarantowanie bezpieczeństwa obywateli jest podstawowym zadaniem państwa. Państwo poprzez powołane instytucje publiczne zabezpiecza prawa obywateli, jak również strzeże ich bezpieczeństwa, także informacyjnego. Każda jednostka organizacyjna w swojej strukturze wprowadza komórki odpowiedzialne za bezpieczeństwo informacyjne. Tworzone są polityki bezpieczeństwa obowiązujące w danych jednostkach, które określają zakres przetwarzanych informacji, sposoby korzystania z nich oraz ochronę.

„Ochrona informacji jest koniecznością i obowiązkiem organizacji; także wymogi prawa nakładają na organizację obowiązek działań o charakterze organizacyjnym oraz technicznym w obszarze ochrony przetwarzanych informacji. Organizacja powinna zapewniać i utrzymywać odpowiedni poziom bezpieczeństwa informacji, dlatego informacje muszą być autentyczne, dostępne tylko dla uprawnionych, dostarczone w odpowiednim czasie i wyłącznie na właściwe stanowiska. Bezpieczeństwo informacji to planowe podejście do ochrony ważnych informacji w celu zapewnienia ich bezpieczeństwa. Obejmuje ludzi, procesy, infrastrukturę i systemy. Bezpieczeństwo informacyjne nie jest stanem stałym i jednorazowym, bo jak pokazuje praktyka musi być systematycznie utrzymywane, weryfikowane i monitorowane. Współczesne środki teleinformatyczne i oprogramowanie komputerowe powodują, że zmagania o informację nabierają szczególnego znaczenia"[4].

Informacje są klasyfikowane według określonych grup lub kategorii. Do pierwszej z nich zalicza się informacje ogólne, takie jak wiadomości przekazywane w środkach masowego przekazu. W celach informacyjnych można upowszechniać informacje o aktualnych wydarzeniach, aktualne artykuły na tematy bieżące, informacje

2. Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. nr 78 poz. 483 ze zm.
3. Ibidem, art. 5.
4. I. Oleksiewicz, W. Krztoń, *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Warszawa, Rambler Press, 2017, s. 27–28.

polityczne lub religijne, wypowiedzi i zdjęcia reporterów, a także przemówienia osób publicznych. W zakres powyższej grupy wchodzą wszelkie utwory nadawane poprzez radio lub telewizję.

Do grupy informacji jawnych kwalifikuje się także informację publiczną, która na podstawie Ustawy z 6 września 2001 r. o dostępie do informacji publicznej stanowi, że jest nią każda informacja o sprawach publicznych. Ustawa ta określa katalog informacji, które mają charakter publiczny[5]. Zgodnie z art. 8 ww. ustawy został utworzony urzędowy publikator teleinformatyczny – Biuletyn Informacji Publicznej, który służy do powszechnego udostępniania informacji publicznej. Oczywiście ustawa przewiduje także możliwość nieudostępnienia informacji publicznej na podstawie przepisów o ochronie informacji niejawnych oraz innych tajemnic ustawowo chronionych.

Kolejną grupą są informacje prawnie chronione, do których zalicza się dwie grupy informacji: informacje szczególne, takie jak dane osobowe, oraz informacje wrażliwe, czyli tajemnice zawodowe. Dane osobowe to grupa informacji umożliwiających zidentyfikowanie osoby fizycznej[6]. Ustawa nie określiła szczegółowo, jakie informacje zalicza się do danych osobowych, jednakże wskazała, że mogą to być wszelkie dane, które pozwolą na powiązanie ich z określoną osobą. Są więc to informacje, które pozwalają na ustalenie tożsamości danej osoby. „Wykorzystuje się do tego celu łatwo osiągalne i popularne źródła. Identyfikacji osoby można dokonać na dwa sposoby: pośrednio lub bezpośrednio, tj. za pomocą informacji takich jak: numer identyfikacyjny, cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe oraz społeczne”[7]. Dane osobowe mogą być przetwarzane tylko w ściśle określonym celu oraz za zgodą osoby, której one dotyczą. Wyróżnia się kilka kategorii tych danych. Są to:

1) „podane dane osobowe – dane osobowe świadomie podane przez osoby fizyczne, np. przy wypełnianiu formularza online;
2) zaobserwowane dane osobowe – dane osobowe rejestrowane automatycznie, np. za pomocą plików cookies lub czujników online, lub telewizji przemysłowej umożliwiającej rozpoznanie twarzy;
3) pochodne dane osobowe – dane osobowe „tworzone” z innych danych w stosunkowo prosty i bezpośredni sposób, np. przy obliczaniu zdolności kredytowej klienta;

Wywnioskowane dane osobowe – dane osobowe tworzone za pomocą bardziej złożonych metod analitycznych (np. poprzez odszukiwanie korelacji między zestawami danych i wykorzystanie tych korelacji do kategoryzacji lub profilowania przyszłych

5. Ustawa z 6 września 2001 r. o dostępie do informacji publicznej, Dz. U. 2022 poz. 902.
6. Ustawa z 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2019 poz. 1781, art. 6 ust. 1.
7. S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki-Organizacji-Państwa.*, Wydanie II, Warszawa, CeDeWu, 2019, s. 198.

wyników zdrowotnych). Dane wywnioskowane są oparte na prawdopodobieństwach i w związku z tym są mniej pewne niż dane pochodne”[8].

Jak wcześniej wspomniano, do informacji wrażliwych zalicza się tajemnice zawodowe, które można pozyskać w czasie pełnienia określonej funkcji lub wykonywania danego zawodu. Do katalogu takich informacji można zaliczyć: tajemnicę dziennikarską, medyczną, handlową, bankową czy przedsiębiorstwa. Odrębną kategorię danych, które podlegają szczególnej ochronie, stanowią informacje niejawne. Informacje te odnoszą się w szczególności do szeroko rozumianego bezpieczeństwa państwa, posiadają własną klasyfikację oraz wynikające z niej klauzule tajności. W ustawie o ochronie informacji niejawnych zostały określone cztery klauzule: „ściśle tajne”, „tajne”, „poufne” oraz „zastrzeżone”[9].

Zgodnie z definicjami określonymi w Ustawie z 5 sierpnia 2010 roku o ochronie informacji niejawnych klauzulę:

- „ściśle tajne” stosuje się do informacji niejawnych, których ujawnienie spowoduje wyjątkowo poważną szkodę Rzeczypospolitej Polskiej, np. zagrozi niepodległości, suwerenności lub integralności terytorialnej RP, zagrozi bezpieczeństwu wewnętrznemu czy osłabi gotowość obronną państwa;
- „tajne” oznacza się informacje niejawne, których ujawnienie mogłoby wyrządzić poważną szkodę Rzeczypospolitej Polskiej – na przykład pogorszyć jej stosunki międzynarodowe, zakłócić przygotowania obronne lub spowodować duże straty w interesach ekonomicznych państwa;
- „poufne” otrzymują informacje niejawne, których nieuprawnione ujawnienie spowoduje szkodę Rzeczypospolitej Polski poprzez np. utrudnienie polityki zagranicznej państwa, zagrozi bezpieczeństwu obywateli czy utrudni wykonywanie zadań służbom ochrony bezpieczeństwa kraju;
- natomiast najniższą klauzulę „zastrzeżone” otrzymują informacje niejawne, które nie mają wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki zasad w zakresie m.in. obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego czy przestrzegania prawa i wolności obywateli.

Dla każdej z powyższych klauzul tajności zostały określone wymagania, które muszą być spełnione dla zapewnienia ochrony informacji niejawnych przed ujawnieniem. Wybór i nadanie klauzuli dla danych dokumentów dokonuje osoba, która jest uprawniona do ich podpisania. Takie dokumenty udostępnia się wyłącznie osobom uprawnionym, które posiadają odpowiednie poświadczenie bezpieczeństwa, otrzymane po pomyślnym

8. M. Gumularz, P. Kozik, *Ochrona danych osobowych. Kontrola i postępowanie w sprawie naruszenia przepisów. Poradnik ze wzorami*, Wydanie II, Warszawa , Wolters Kluwer, 2022, s. 24.
9. Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. 2024 poz. 632 ze zm.

przeprowadzeniu określonego w ustawie postępowania sprawdzającego i odbyciu szkolenia z zakresu ochrony informacji niejawnych. Udostępnienie tych dokumentów ograniczone jest tylko do niezbędnego zakresu, związanego ściśle z wykonywaną pracą na danym stanowisku. Wymogiem jest także, aby takie udostępnienie następowało w warunkach, które uniemożliwiają ich nieuprawnione ujawnienie, np. w kancelariach tajnych lub innych pomieszczeniach spełniających wymagania określone w ustawie i przepisach wykonawczych. Wyróżnia się także podział informacji dokonywany pod kątem kryteriów jakości związanych z ich ochroną, takich jak:

1) „tajność – informuje o wymaganym stopniu ochrony informacji przed nieuprawnionym dostępem; stopień tajności jest uzgadniany przez osoby lub organizacje dostarczające i otrzymujące informację;
2) integralność – oznacza, że na informacji nie zostały wykonane niedozwolone działania;
3) dostępność – oznacza wymagany przez użytkownika (lub zapisany w wymaganiach stawianych systemowi przetwarzania informacji) stopień dostępności danych, procesów i aplikacji;
4) rozliczalność – określa możliwość identyfikacji użytkowników informacji i systemu teleinformatycznego oraz wykorzystanych przez nich usług; kryterium to decyduje także o możliwości prowadzenia skutecznej analizy powłamaniowej;
5) niezaprzeczalność – informacje o możliwości wyparcia się uczestnictwa przez podmiot uczestniczący w wymianie informacji;
6) autentyczność – oznacza możliwość jednoznacznego stwierdzenia, jaki podmiot przesłał dane”[10].

Kryteria powyższe zależą głównie od samej informacji, jak również od przyjętych rozwiązań organizacyjnych i technicznych systemu, który je przetwarza.

W społeczeństwie informacyjnym informacja stała się siłą napędową współczesnego społeczeństwa, postrzeganą jako surowiec, towar i produkt na sprzedaż. Obecnie ma ona niezwykle ważną rolę społeczną, a jej siła ma wpływ zarówno na życie osobiste, jak i zawodowe człowieka.

„Jedną z najważniejszych kwestii ochrony bezpieczeństwa jest opracowanie przez organizację polityki bezpieczeństwa informacji. Jest to udokumentowany zbiór zasad, praktyk i procedur, w którym dana organizacja określa, w jaki sposób chroni aktywa systemu informacyjnego oraz przetwarzanie informacji. Jest to dokument, który wskazuje na zaangażowanie kierownictwa w bezpieczeństwo informacji, a także określa, jaki wpływ na realizację i wspieranie wizji i misji organizacji ma bezpieczeństwo informacji. Opracowanie polityki bezpieczeństwa przebiega w kilku etapach, na które składają się:

10. K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydanie II, Warszawa, PWN, 2017, s. 17.

– analiza potrzeb – określenie zagrożeń, oszacowanie potencjalnych strat, inwentaryzacja systemu informacyjnego, zdefiniowanie wymagań, analiza możliwych rozwiązań, określenie optymalnego sposobu inwestowania;
– definiowanie polityki bezpieczeństwa – określenie celów, wyznaczenie zależności, określenie przepływów informacyjnych, opublikowanie zasad bezpieczeństwa, zaplanowanie szkoleń, sposobów monitorowania i kontroli stosowania polityki bezpieczeństwa;
– wdrażanie polityki bezpieczeństwa – opublikowanie polityki bezpieczeństwa, powołanie zespołów, przydzielenie prac, weryfikacja znajomości polityki bezpieczeństwa, szkolenia praktyczne, informowanie o istotnych wydarzeniach i zmianach;
– kontroling, monitoring bezpieczeństwa – konfrontacja rzeczywistości z zaplanowaną polityką, audyt bezpieczeństwa, przegląd wydarzeń związanych z bezpieczeństwem, monitorowanie aktywności systemu, gromadzenie i analiza informacji, sprawdzanie poziomu znajomości zasad bezpieczeństwa przez pracowników”[11].

Każdy z powyższych elementów ma wpływ na jakość prowadzonej Polityki bezpieczeństwa informacji. Może wydawać się, że przygotowanie ww. dokumentu nie stanowi wyzwania dla przedsiębiorstwa czy instytucji. Niestety jest to bardzo mylne założenie. W dobie społeczeństwa informacyjnego, szybkości zachodzących zmian oraz błyskawicznego rozwoju nowych form komunikacji, bardzo ważne jest wprowadzenie właściwie przygotowanej Polityki bezpieczeństwa zawierającej wszystkie niezbędne elementy ochrony informacji.

Rozporządzenie o ochronie danych osobowych, czyli RODO

Od 1997 roku w Polsce funkcjonuje Ustawa o ochronie danych osobowych (UODO), która reguluje zasady przetwarzania danych osobowych oraz obowiązki administratora danych. Ustawa została wprowadzona w zawiązku z koniecznością wdrożenia zapisów dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[12].

11. S. Wojciechowska-Filipek, Z. Ciekanowski, op. cit., s. 157.
12. G.P. Wójcik, *Obowiązki przedsiębiorców wynikające z RODO*, Wydanie I, Warszawa, CeDeWu, 2021, s. 13.

Jednak dopiero uchylenie ww. dyrektywy i „wejście w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Rozporządzenie RODO) wywołało wstrząs społeczny[13]".

„Obowiązujące od 21 lat zasady przetwarzania danych osobowych nie zostały zastąpione, lecz zaktualizowane i istotnie wzmocnione. (...). System ochrony nadal opiera się na podstawowych zasadach, takich jak zasady celowości, adekwatności czy ograniczenia czasowego, nadal wymaga wykazania podstawy prawnej przetwarzania i zwiększa rygoryzm tego wymogu w stosunku do danych wrażliwych, nadal przyznaje osobie, której dane dotyczą, prawo dostępu do nich, korygowania ich i sprzeciwu wobec ich przetwarzania itd. Jednak elementy tej konstrukcji zostały zmodernizowane ze względu na rosnący wpływ Internetu i nowych technologii na ochronę danych osobowych"[14].

Rysunek 1. Dziesięć najważniejszych zmian wprowadzonych przez RODO

1. Bezpośrednia odpowiedzialność przetwarzającego dane
2. Zgłoszenie naruszeń
3. Nowe i rozszerzone prawa obywateli
4. Ograniczenia profilowania
5. Wyznaczenie inspektora ochrony danych
6. Inwentaryzacja danych i wymagania wobec dokumentacji
7. Zgody
8. Rozbudowanie obowiązku informacyjnego
9. Ocena wpływu ochrony danych
10. Transfer danych poza Unię Europejską

Źródło: G.P. Wójcik, Obowiązki przedsiębiorców wynikające z RODO, Wydanie I, Warszawa, CeDeWu, 2021, s. 17.

„Coraz większe znaczenie zyskuje zatem zapewnienie właściwej ochrony przetwarzanych danych, w szczególności danych osobowych. Ich przetwarzanie może bowiem powodować negatywne konsekwencje dla społeczeństwa (zbiorowości) i dla jego poszczególnych członków.

13. A. Sobczak, *RODO Rozproszona władza publiczna, Wydanie I,* Kraków, Wyd. Uniwersytetu Jagiellońskiego, 2019, s. 11.
14. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i rady (UE) 2016/679*, Warszawa, C.H. Beck, 2016, s. 6.

Ataki cybernetyczne skutkujące wyciekiem danych do sieci, rozwój przestępczości cybernetycznej, wykradanie tożsamości, nielegalna sprzedaż danych do celów marketingowych oraz niekontrolowane i niezgodne z prawem przetwarzanie tych danych, to tylko niektóre ze zjawisk szkodliwych społecznie, których eliminowanie jest w interesie publicznym. (...).

Zapewnienie ochrony danych osobowych ma również istotne znaczenie dla osób fizycznych. Wpływa ono bowiem na skuteczność realizacji prawa do prywatności. Prawo to obejmuje zasady i reguły odnoszące się do różnych sfer życia jednostki, a ich wspólnym mianownikiem jest przyznanie jednostce prawa do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[15].

W Polsce przepisy zaczęły być stosowane bezpośrednio od 25 maja 2018 roku. Ustanowiono nowy organ właściwy w sprawie ochrony danych osobowych – Prezesa Urzędu Ochrony Danych Osobowych (PUODO), który zastąpił dotychczasowy organ nadzoru – Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Każdego przedsiębiorcę unijnego mającego do czynienia z danymi osobowymi, obowiązuje RODO. Za przestrzeganie tych zasad odpowiedzialny jest Administrator, czyli jednostka organizacyjna, która decyduje o celach i środkach przetwarzania danych osobowych – w niniejszej pracy będzie to Kasa Rolniczego Ubezpieczenia Społecznego (KRUS). Jest to instytucja powołana Ustawą z 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników[16], która zgodnie z art. 2 ust. 1 przedmiotowej ustawy określiła, że Kasa realizuje ubezpieczenie społeczne rolników. Kasą Rolniczego Ubezpieczenia Społecznego kieruje Prezes – centralny organ administracji rządowej.

Dobrą praktyką jest wyznaczenie inspektora ochrony danych (IOD). W rozporządzeniu RODO brak jest definicji wyżej wskazanej funkcji, a zapisy obejmują tylko jego miejsce w strukturze przedsiębiorstwa oraz należące do niego zadania.

W przedsiębiorstwie powinny obowiązywać wewnętrzne uregulowania dotyczące ochrony danych osobowych, które muszą określać zastosowane środki bezpieczeństwa, służące utrzymaniu integralności, poufności i rozliczalności danych, a także dostępności systemów i usług przetwarzania.

W Kasie Rolniczego Ubezpieczenia Społecznego wprowadzono – zarządzeniem nr 15 Prezesa KRUS z 9 lipca 2024 r. – Politykę bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcję zarządzania systemami informatycznymi, służącymi

15. M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych,* Wrocław, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2018, s. 21.
16. Ustawa z 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników, Dz.U. 2024 poz. 90 ze zm.

do przetwarzania danych osobowych w KRUS i określającymi zasady, procedury i odpowiedzialność w zakresie ochrony danych osobowych.

Zgodnie z rozporządzeniem RODO „każdy podmiot musi samodzielnie oceniać ryzyko, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą. To właśnie te wartości należy przede wszystkim brać pod uwagę”[17].

RODO „nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie. Każdy podmiot musi dokonywać jej samodzielnie, uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne czy zakres i rodzaj danych oraz cel ich przetwarzania. Jednym ze skutecznych systemowych sposobów dokonywania oceny ryzyka jest wdrożenie w danej jednostce procesu zarządzania ryzykiem”[18].

Na tym etapie warto zwrócić uwagę na znaczenie ochrony danych osobowych w szczególnie wymagających warunkach, jakie przyniosła pandemia COVID-19, w związku ze wzrostem liczby osób pracujących zdalnie.

Zacznijmy od najważniejszego – praca zdalna nie zwalnia z przestrzegania zasad RODO. „RODO pozwala właściwym organom ds. zdrowia publicznego i pracodawcom na przetwarzanie danych osobowych w kontekście epidemii, zgodnie z prawem krajowym i na określonych w nim warunkach (…)”[19]. Praca zdalna jest możliwa i posiada podstawy prawne, ale aby zabezpieczyć obszary ochrony danych osobowych, niezbędne jest przestrzeganie ustalonych standardów i zaleceń.

Urząd Ochrony Danych Osobowych przedstawił wytyczne dotyczące bezpieczeństwa danych osobowych podczas pracy poza biurem. Dotyczą one użytkowania urządzenia, e-maila oraz dostępu do sieci i chmury. Należy pamiętać, że urządzenia i oprogramowanie przekazane przez pracodawcę służą tylko i wyłącznie do wykonywania obowiązków służbowych. Należy zawsze postępować zgodnie z przyjętą w organizacji procedurą bezpieczeństwa[20].

Praca zdalna niesie za sobą szereg obowiązków w obszarze ochrony danych osobowych. Należy również pamiętać o zapewnieniu przestrzegania przepisów RODO. Dotyczy to zarówno pracownika, jak i pracodawcy. Jedynie rygorystyczne przestrzeganie zasad i wytycznych zapewni pełne bezpieczeństwo pracy i nie narazi nikogo na ryzyko utraty lub wycieku danych.

17. UODO, https://uodo.gov.pl/pl/126/208, dostęp 7.02.2025.
18. Ibidem.
19. UODO, https://uodo.gov.pl/pl/138/1463, dostęp 26.04.2022; Oświadczenie Przewodniczącej Europejskiej Rady Ochrony Danych, Andrea Jelinek w sprawie przetwarzania danych osobowych w kontekście pandemii COVID-19 z 19 marca 2020 r.
20. UODO, https://uodo.gov.pl/pl/138/1459, dostęp 26.04.2022.

Ochrona danych osobowych w Kasie Rolniczego Ubezpieczenia Społecznego

Na podstawie art. 59 ust. 3 Ustawy z 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników oraz art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz. Urz. UE. L. Nr 119, str. 1) w KRUS wprowadzono zarządzeniem nr 15 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 roku:

1. Politykę bezpieczeństwa w zakresie ochrony danych osobowych KRUS.
2. Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Kasie Rolniczego Ubezpieczenia Społecznego[21].

Dokumenty te są ważnymi wytycznymi mającymi na celu zapewnienie przestrzegania przepisów prawa unijnego i krajowego dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

Dodatkowo dla zapewnienia właściwej ochrony pozostałym zasobom informacyjnym Kasy opracowano i wprowadzono w życie Politykę Bezpieczeństwa Informacji, której podstawowym zadaniem jest ochrona aktywów poprzez utrzymanie, doskonalenie i rozwój systemu zarządzania bezpieczeństwem informacji (zwany w Kasie Zintegrowanym Systemem Zarządzania), dzięki któremu łatwiej zidentyfikować zagrożenia oraz zminimalizować ryzyko utraty informacji. System funkcjonuje we wszystkich jednostkach i komórkach organizacyjnych Kasy i jest zgodny z wymaganiami:

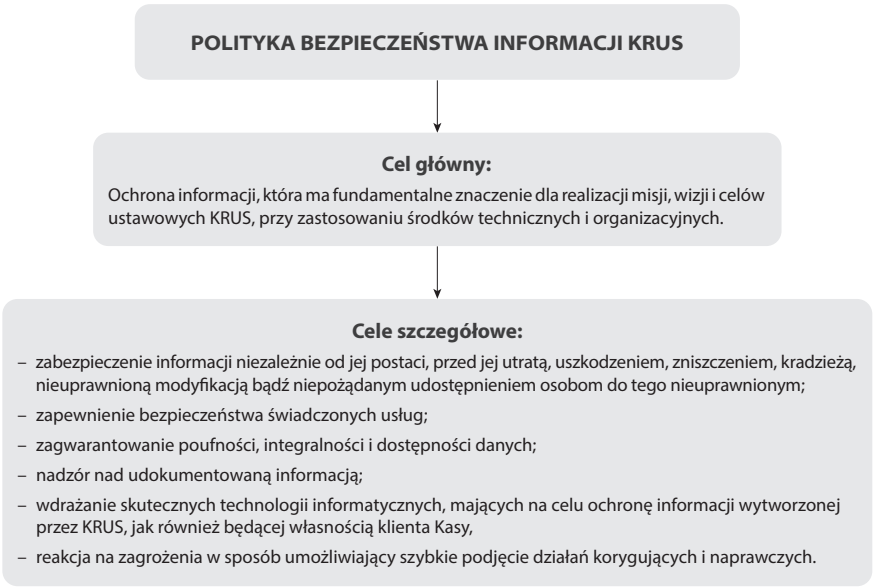
1) norm: ISO 9001, ISO/IEC 27001 i ISO 37001, Zarządzeniem nr 3 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 2 lutego 2023 r. w sprawie utrzymania i doskonalenia w Kasie Rolniczego Ubezpieczenia Społecznego Zintegrowanego Systemu Zarządzania na podstawie wymagań obowiązujących norm: ISO 9001, ISO/IEC 27001 i ISO 37001 oraz określenia zakresu odpowiedzialności w ramach Zintegrowanego Systemu Zarządzania;
2) standardów kontroli zarządczej dla sektora finansów publicznych.

Warto zaznaczyć, że do wspomnianego systemu dostęp mają wszyscy pracownicy Kasy, co pozwala im na bieżąco zapoznawać się z nowymi wytycznymi, sprawdzać obowiązujące przepisy prawa wewnętrznego oraz dwa razy do roku realizować wymóg

21. Zarządzenie Nr 15 Prezesa Kasy rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r. w sprawie wprowadzenia w Kasie Rolniczego Ubezpieczenia Społecznego Polityki bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, Dz. Urz. KRUS 2024 poz. 16.

zdawania testów mających na celu weryfikację posiadanej wiedzy z zakresu realizowanych zadań i obowiązujących procedur.

Rysunek 2. Cele Polityki bezpieczeństwa KRUS



Źródło: Opracowanie własne na podstawie Księgi Zintegrowanego Systemu Zarządzania KRUS, Wydanie XXIII, 1 października 2024 roku.

Osobą odpowiedzialną za wykonywanie obowiązków z zakresu przetwarzania i ochrony danych osobowych jest Inspektor Ochrony Danych (IOD) – tj. Dyrektor Biura Zarządzania Kryzysowego, Spraw Obronnych i Bezpieczeństwa Informacji Centrali KRUS, którego powołuje Prezes Kasy. Do zadań IOD należy:

1) „informowanie Administratora Danych (Kasę Rolniczego Ubezpieczenia Społecznego) i pracowników, którzy przetwarzają dane osobowe, o obowiązkach wynikających z przetwarzania danych osobowych oraz doradzanie im w tym zakresie;
2) monitorowanie przestrzegania przepisów o ochronie danych osobowych, w tym Polityki bezpieczeństwa i Instrukcji, a także podział obowiązków oraz działania zwiększające świadomość;
3) udzielanie zaleceń co do oceny skutków dla ochrony danych i monitorowanie wykonania ochrony danych, przeprowadzanie inspekcji w oddziałach regionalnych Kasy w tym zakresie;
4) opracowywanie wytycznych i zaleceń w zakresie ochrony danych osobowych;

5) współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, a także w stosowanych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
6) opracowywanie i aktualizowanie Polityki bezpieczeństwa i Instrukcji oraz przestrzeganie zasad w nich określonych;
7) prowadzenie zbiorczego wykazu zbiorów danych osobowych przetwarzanych w Kasie"[22].

Inspektor Ochrony Danych gromadzi dokumentację z przeprowadzonych w KRUS analiz ryzyka dotyczących zidentyfikowanych ryzyk odnośnie ochrony danych osobowych, planów minimalizacji tych ryzyk, podnosi świadomość pracowników KRUS odnośnie ryzyk i incydentów bezpieczeństwa dotyczących ochrony danych osobowych. IOD prowadzi zbiorczy rejestr danych w Kasie, który to otrzymuje rejestry zbiorów danych od Koordynatora Bezpieczeństwa Informacji – KBI (którym jest każdy dyrektor oddziału regionalnego KRUS) oraz od Koordynatora Zbioru Danych Osobowych – KZDO (którym jest każdy kierownik komórki organizacyjnej w Centrali Kasy). Rejestr prowadzony jest w formie elektronicznej lub papierowej.

Z kolei do zadań KBI i KZDO m.in. należy:

1) „organizacja przetwarzania i dbanie o bezpieczeństwo danych osobowych poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych zaprojektowanych w celu skutecznej realizacji zasad ochrony danych i w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane osobowe dotyczą;
2) wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzane były tylko te dane osobowe, które są niezbędne do osiągnięcia każdego konkretnego celu przetwarzania;
3) poprzez proces zarządzania ryzykiem prowadzenie systematycznej oceny, czy stopień bezpieczeństwa jest odpowiedni, uwzględniający ryzyko związane z przetwarzaniem danych osobowych, w szczególności wynikające z przypadkowego, niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia, nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
4) podejmowanie decyzji o udostępnieniu danych osobowych innym osobom lub podmiotom;

22. Polityka bezpieczeństwa w zakresie ochrony danych osobowych Kasy Rolniczego Ubezpieczenia Społecznego, załącznik nr 1 do zarządzenia nr 15 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r.

5) w przypadku powierzenia administrowanych danych innemu podmiotowi, przygotowanie projektu, a następnie zawarcie umowy o powierzenie przetwarzania danych osobowych;
6) zgłaszanie do IOD zbiorów danych osobowych, w których przetwarzane są dane osobowe, a których jest koordynatorem oraz potrzebę ich aktualizacji lub wykreślenia;
7) niezwłoczne informowanie, zgodne z procedurą określoną w Zintegrowanym Systemie Zarządzania, zwanym dalej „ZSZ", IOD o stwierdzonych nieprawidłowościach i incydentach w zakresie ochrony danych osobowych w administrowanych zbiorach;
8) współpraca z IOD w zakresie doskonalenia metod oraz sposobów zabezpieczania i ochrony zbiorów danych osobowych;
9) nadzorowanie zasad ochrony, przechowywania i niszczenia kopii bezpieczeństwa zbiorów danych osobowych; (…);
10) przekazywanie do IOD, w terminie do 20 stycznia, sprawozdania za rok poprzedni, uwzględniającego liczbę, zakres tematyczny, a także odbiorców, którym udostępniono przetwarzane dane osobowe;
11) nadawanie, modyfikowanie i odwoływanie upoważnień osobom do przetwarzania danych osobowych w powierzonych systemach/zbiorach. (…);
12) prowadzenie:
    – Rejestru osób upoważnionych do przetwarzania danych osobowych w zbiorach;
    – Rejestru upoważnień wydanych Administratorowi Systemów Informatycznych (ASI);
    – Rejestru osób upoważnionych do wykonywani funkcji ASI (…);
    – Rejestru zbiorów danych osobowych przetwarzanych w Kasie (…);
    – Rejestru czynności przetwarzania (…) oraz przekazywanie go po bieżącej aktualizacji do IOD;
    – Rejestru udostępnienia danych osobowych (…);
    – Wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe oraz przekazywanie go po bieżącej aktualizacji do IOD"[23].

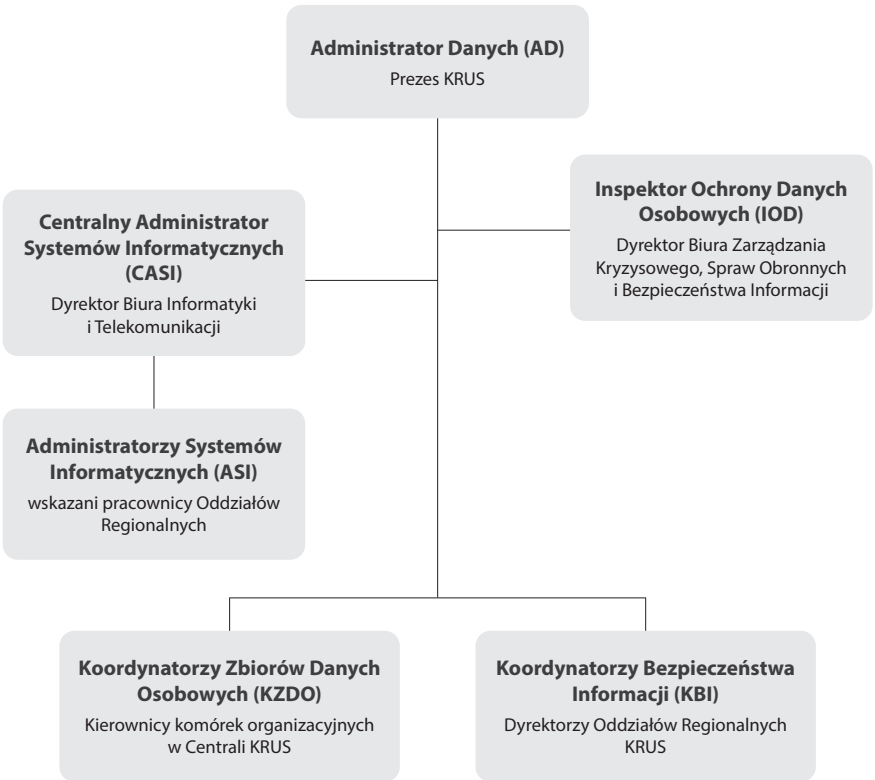
Tak szeroki zakres działania dyrektorów oddziałów regionalnych Kasy pozwala na należyte wykonywanie czynności służbowych z zakresu bezpieczeństwa informacji, jak również ochrony danych osobowych. Należy pamiętać, że jednostki organizacyjne KRUS, jakimi są oddziały regionalne i podlegające im placówki terenowe Kasy, są głównym miejscem kontaktu pracowników z klientami zewnętrznymi Kasy, czyli zarówno ubezpieczonymi, świadczeniobiorcami, jak i wykonawcami zadań zleconych.

23. Ibidem.

Dlatego też tak ważne jest, aby osoby pełniące funkcję KBI właściwie wykonywały nałożone na nich czynności.

Przedstawione powyżej zadania realizowane są, jak już wspomniano, przez kierowników komórek organizacyjnych w Centrali Kasy, czyli dyrektorów biur merytorycznych i pełnomocników Prezesa powołanych do kierowania wskazanymi zespołami. Praca wykonywana w ramach pełnionych przez nich obowiązków także powinna uwzględniać wymogi polityki bezpieczeństwa KRUS.

Rysunek 3. Struktura funkcji przypisanych w ramach Polityki bezpieczeństwa KRUS



Źródło: Opracowanie własne na podstawie Zarządzenia nr 15 Prezesa KRUS z 9 lipca 2024 r. w sprawie wprowadzenia w Kasie Rolniczego Ubezpieczenia Społecznego Polityki bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Z uwagi na fakt, że przetwarzanie danych osobowych w dużej mierze odbywa się przy zastosowaniu programów i systemów informatycznych przeznaczonych do tego, warto tutaj wspomnieć także o dwóch ważnych funkcjach: CASI i ASI. Prezes Kasy

wyznaczył Dyrektora Biura Informatyki i Telekomunikacji Centrali Kasy na Centralnego administratora systemów informatycznych. CASI głównie:

1) „odpowiada za zarządzanie centralnymi systemami informatycznymi, w szczególności implementację w systemach reguł wynikających z przepisów prawa, a w przypadku usług informatycznych świadczonych przez podmioty zewnętrzne, zapewnienie i przygotowanie projektu umów o powierzenie przetwarzania danych osobowych;
2) organizuje i koordynuje szkolenia osób przewidzianych do realizowania zadań administratora systemów informatycznych w zakresie danych osobowych przetwarzanych w formie elektronicznej z wykorzystaniem systemu informatycznego;
3) prowadzi nadzór merytoryczny nad pracami ASI zatrudnionymi w Centrali Kasy;
4) wydaje wytyczne i wskazówki techniczne dla ASI w jednostkach organizacyjnych Kasy”[24].

Osoby wyznaczone na administratorów systemów informatycznych nadzorują prawidłowe funkcjonowanie systemów, stąd każdy „ASI odpowiada za eksploatację systemów informatycznych, a w szczególności za:

1) bieżące utrzymanie i modernizację infrastruktury techniczno-systemowej;
2) rejestrowanie i wyrejestrowywanie użytkowników z systemu informatycznego;
3) przydzielanie uprawnień do poszczególnych funkcji;
4) określenie trybu i częstotliwości zmiany haseł oraz reguł ich tworzenia;
5) wykonywanie procedury kopii bezpieczeństwa oraz ich właściwe przechowywanie, sprawdzanie poprawności zapisu i ich niszczenie;
6) wdrożenie stosowanych procedur w sytuacji naruszenia ochrony danych osobowych;
7) przeprowadzenie szkoleń osób przewidzianych do realizowania zadań związanych z przetwarzaniem danych osobowych z zakresu ochrony danych osobowych przetwarzanych w formie elektronicznej z wykorzystywaniem systemu informatycznego, z uwzględnieniem przepisów wewnętrznych obowiązujących w Kasie”[25].

Obie te ważne funkcje, pozwalają na zapewnienie i nadzorowanie właściwej ochrony systemów informatycznych. Bezpieczeństwo informacji musi obejmować swoim zakresem wspomniane już aktywa systemu informacyjnego oraz przetwarzanie informacji w nich zawartych.

Jak zapisano w rozporządzeniu RODO, każda organizacja sama ocenia ryzyko dotyczące osób, których dane są przez nią przetwarzane. Tym samym ważne jest postępowanie zgodnie z ustalonymi zasadami.

24. Ibidem.
25. Ibidem.

Na tej podstawie Kasa Rolniczego Ubezpieczenia Społecznego przetwarza dane osobowe zgodnie z takimi zasadami jak:

1) zasada zgodności z prawem, rzetelności i przejrzystości;
2) zasada ograniczonego celu;
3) zasada minimalizacji danych;
4) zasada prawidłowości;
5) zasada ograniczonego przechowywania;
6) zasada integralności i poufności.

Osoba, której dane osobowe są przetwarzane w KRUS, ma prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do cofnięcia zgody w dowolnym momencie na dalsze przetwarzanie danych w przypadku, gdy ich przetwarzanie wymaga takiej zgody, oraz prawo do wniesienia skargi do organu nadzorczego (tj. do Prezesa Urzędu Ochrony Danych osobowych – PUODO), jeśli uzna, że jej dane osobowe przetwarzane są niezgodnie z ogólnym rozporządzeniem o ochronie danych osobowych[26].

Zdarzenia naruszające ochronę danych osobowych należy bez zbędnej zwłoki zgłosić organowi nadzorczemu, o czym decyduje AD, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Jednostki organizacyjne Kasy, jako podmioty przetwarzające dane osobowe, zgłaszają IOD naruszenie ochrony danych osobowych.

Zgodnie z zapisami zarządzenia Inspektor Ochrony Danych jest zobowiązany do dokumentowania wszelkich zdarzeń naruszenia ochrony danych osobowych oraz działań, jakie zostały podjęte, żeby w przyszłości wyeliminować podobne zdarzenia.

„Każdy pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie i na nośnikach tradycyjnych, zobowiązany jest do niezwłocznego poinformowania o tym przełożonego lub właściwego dla danego systemu ASI lub KBI, KZDO, CASI, którzy powiadamiają IOD, a ten z kolei powiadamia AD”[27]. Następnie po identyfikacji i potwierdzeniu incydentu przeprowadza się postępowanie wyjaśniające i podejmuje działania naprawcze.

Nałożenie obowiązków na pracowników Kasy, gwarantuje szybkie wykrycie naruszenia oraz umożliwia lepszą weryfikację ewentualnych uchybień. Przeprowadzenie działań naprawczych ma za zadanie wyeliminowanie powstałych sytuacji w dalszej pracy jednostki Kasy.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych Kasy Rolniczego Ubezpieczenia Społecznego zobowiązuje także wszystkie swoje jednostki organizacyjne do opracowania wykazu budynków, pomieszczeń lub części pomieszczeń

26. Ibidem.
27. Ibidem.

tworzących obszar, w których przetwarzane są dane osobowe. Taki zbiorczy wykaz prowadzi Inspektor Ochrony Danych w KRUS.

Dla zapewnienia fizycznego bezpieczeństwa przetwarzanym danym w Centrali Kasy oraz w oddziałach regionalnych i podległych placówkach terenowych Kasy stosuje się kontrolę dostępu do budynków i pomieszczeń, w których przetwarzane są dane osobowe.

Nad prawidłowym jej działaniem w Centrali Kasy taki nadzór sprawuje Dyrektor Biura Administracji i Inwestycji, a w oddziałach regionalnych i podległych placówkach terenowych Kasy – KBI. Ponadto wszystkich pracowników KRUS obowiązuje znajomość „Instrukcji podstawowych zasad bezpieczeństwa dla pracowników KRUS"[28], która obejmuje podstawowe zasady bezpieczeństwa informacji przetwarzanych przez KRUS obowiązujące podczas codziennej pracy. Kontrola wejść do budynków i pomieszczeń w dużej mierze utrudnia dostęp osób nieupoważnionych do danych, które nie powinny być ujawniane osobom niemającym do tego uprawnień.

Jak już wspomniano, załącznikiem nr 2 do zarządzenia nr 15 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r. jest Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Kasie Rolniczego Ubezpieczenia Społecznego, która została opracowana w celu określenia zasad przetwarzania danych osobowych w systemach informatycznych wykorzystywanych w Kasie. W związku z powyższym Biuro Informatyki i Telekomunikacji Centrali Kasy opracowało szereg procedur, które zostały opublikowane w Zintegrowanym Systemie Zarządzania KRUS.

Pracownicy Kasy Rolniczego Ubezpieczenia Społecznego jako użytkownicy systemów przetwarzających dane osobowe w Kasie muszą posiadać unikalny identyfikator i hasło w celach uwierzytelniania oraz kontroli dostępu do danych. Wszystkie dane osobowe przetwarzane w systemach informatycznych Kasy przechowywane są na elektronicznych nośnikach informacji, które charakteryzują się trwałością zapisu. Za prawidłowość przechowywania i oznakowania nośników informacji zawierających dane osobowe odpowiadają: CASI – w Centrali KRUS, a w oddziale regionalnym i placówkach terenowych Kasy – KBI, którzy to wykonują ich kopie bezpieczeństwa.

„W razie stwierdzenia lub podejrzenia zaistnienia zdarzenia zagrażającego bezpieczeństwu systemu informatycznego należy postąpić zgodnie z procedurami obowiązującymi w Kasie"[29].

28. Instrukcja podstawowych zasad bezpieczeństwa dla pracowników KRUS, Wydanie XV, 16 sierpnia 2021 r.
29. Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Kasie Rolniczego Ubezpieczenia Społecznego, załącznik nr 2 do zarządzenia nr 17 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 24 maja 2018 r.

Wszystkie opisane powyżej zasady, procedury i formy postępowania z danymi osobowymi mają na celu właściwe zabezpieczenie dostępu do tych danych, ich prawidłowe przetwarzanie oraz przechowywanie z ograniczonym dostępem – wyłącznie dla upoważnionych pracowników Kasy Rolniczego Ubezpieczenia Społecznego.

Podsumowanie

„Zagrożenia bezpieczeństwa społeczeństwa informacyjnego są zagrożeniami realnymi, obecnymi w codziennej rzeczywistości życia podmiotu, zatem zapoznanie, osiągnięcie, utrzymanie i doskonalenie bezpieczeństwa informacyjnego staje się nieodzowne do zapewnienia przewagi konkurencyjnej organizacji, płynności finansowej, rentowności, pozostawania w zgodzie z literą prawa”[30].

W ostatnich latach nowego znaczenia nabrało „bezpieczne” przetwarzanie, przechowywanie i przesyłanie informacji. Witryny internetowe takie jak WikiLeaks, jasno wskazują, że nawet skrajnie tajne dokumenty mogą zostać łatwo i szybko, a także anonimowo ujawnione. Dlatego osoby korzystające z udogodnień współczesnej techniki muszą zwracać szczególną uwagę na formy i sposoby przekazywania swoich informacji czy dokumentów. Zaufanie, którym wcześniej obdarzaliśmy aplikacje czy systemy, z których korzystaliśmy bez obaw, już dawno zostało nadwyrężone. Podobna sytuacja pojawia się także u osób odpowiedzialnych za szeroko rozumiane przetwarzanie informacji czy u właścicieli tych informacji, którzy tracą zaufanie do obecnych zabezpieczeń i szukają coraz to nowszych i lepszych sposobów upewnienia się, że ich informacje są bezpieczne. Dane osobowe gromadzone oraz przetwarzane przez organizacje, przedsiębiorstwa i instytucje muszą być chronione nie tylko prawnie, lecz także za pomocą dodatkowych systemów, które zagwarantują ich właściwe użytkowanie i przechowywanie. Żadna z instytucji nie może sobie pozwolić na utratę lub upublicznienie danych swoich klientów – zarówno zewnętrznych, jak i wewnętrznych.

Dlatego też stworzenie właściwej Polityki bezpieczeństwa informacji ma ogromne znaczenie dla instytucji, jaką jest Kasa Rolniczego Ubezpieczenia Społecznego. Jej narzędzia mają pozwolić na właściwe zabezpieczenie informacji. Ważne jest także cykliczne przeprowadzanie oceny istniejących zabezpieczeń, której elementem jest audyt, czyli postępowanie sprawdzające sposób, jak również wynik wykonania pewnych zadań pod względem ich zgodności z określonymi wymaganiami, standardami czy normami. Dowody audytowe zebrane podczas takiej czynności pozwalają na dokonanie oceny, a podjęte kroki, zabezpieczenia systemowe i rozwiązania wprowadzane w instytucji

30. I. Oleksiewicz, W. Krztoń, op. cit., s. 9.

w pełni zabezpieczają przed niewłaściwym wypływem tych informacji, które mają być chronione. Ma to szczególne znaczenie dla ochrony danych osobowych.

Bezpieczeństwo informacji w Kasie Rolniczego Ubezpieczenia Społecznego zostało zapewnione m.in. poprzez opracowanie wewnętrznej regulacji, jaką jest „Polityka bezpieczeństwa informacji Kasy Rolniczego Ubezpieczenia Społecznego". Jej celem jest „wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe podczas ich przetwarzania zarówno w formie papierowej, jak i w systemach informatycznych"[31].

Kluczową funkcję w realizacji ww. działań pełni Inspektor Ochrony Danych KRUS, który w imieniu Administratora Danych – Prezesa Kasy realizuje zadania wynikające z RODO oraz Ustawy z 10 maja 2018 r. o ochronie danych osobowych i dba o prawidłowe funkcjonowanie systemu. Ze względu na wielkość organizacji oraz ilość przetwarzanych danych osobowych Administrator Danych powierzył realizację większości zadań dyrektorom oddziałów regionalnych (KBI) oraz kierownikom komórek organizacyjnych Centrali Kasy – biur i zespołów (KZDO), którzy sprawują nadzór nad działaniami jednostek organizacyjnych Kasy. Przyjęte rozwiązanie pozwoliło na realizację zadań wynikających z RODO i wspomnianej ustawy o ochronie danych osobowych bez zmian struktury organizacyjnej.

Szeroko rozbudowana „Polityka bezpieczeństwa informacji Kasy Rolniczego Ubezpieczenia Społecznego" pozwala stwierdzić, że ochrona danych osobowych jest w tej instytucji właściwie zabezpieczona. Jak wspomniano w poprzednim rozdziale, podstawowym zadaniem tej polityki jest ochrona aktywów poprzez utrzymanie, doskonalenie i rozwój systemu zarządzania bezpieczeństwem informacji (Zintegrowany System Zarządzania), dzięki któremu łatwiej można zidentyfikować zagrożenia oraz zminimalizować ryzyko utraty informacji.

Ważne jest podkreślenie, że Polityka bezpieczeństwa i pochodne jej dokumenty we właściwy i syntetyczny sposób opisują postępowanie z danymi, których ochrona leży w interesie zarówno KRUS, jak i ich klientów zewnętrznych i wewnętrznych.

Samo zabezpieczenie prawne i systemowe nie gwarantuje braku możliwości naruszenia bezpieczeństwa informacji. Dlatego tak ważne jest, aby czynnik ludzki, który może pomyłkowo lub celowo naruszyć ustalone przepisy, został właściwie przeszkolony.

Ciągły rozwój technologii cyfrowych, w tym sztucznej inteligencji, czy nieustanny wzrost znaczenia informacji wymagają bieżącej analizy tematu. A co za tym idzie dokonywania ciągłych aktualizacji bieżących wymagań, jak również zabezpieczeń.

31. Polityka bezpieczeństwa w zakresie ochrony danych osobowych Kasy Rolniczego Ubezpieczenia Społecznego, załącznik nr 1 do zarządzenia nr 15 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r.

W przypadku gdy pojawi się naruszenie zasad bezpieczeństwa informacji, konieczne jest dokonanie analizy takiej sytuacji, wyciągnięcie zarówno konsekwencji, jak i wniosków, a także wprowadzenie koniecznych zmian uniemożliwiających jej ponowne wystąpienie.

W dobie szybko rozwijającego się społeczeństwa informacyjnego pojawia się wiele nowych wyzwań oraz nowych perspektyw. Ważne jest, aby sprostać jak największej liczbie wyzwań. Obecnie najważniejsze z nich to: zagrożenie dla bezpieczeństwa, uniezależnienie od internetu, jak również manipulacja informacją. Konieczne jest, aby perspektywy rozwoju społecznego brały pod uwagę te wyzwania, których całkowite wyeliminowanie nie jest możliwe.

Obecnie trudno jednoznacznie wskazać, które z wyzwań jest najistotniejsze. Dynamiczne zmiany społeczne i nieustanny rozwój świata sprawiają, że przewidzenie przyszłych kierunków tych zmian jest dziś wyjątkowo trudne.

Bibliografia

Aleksandrowicz T.R., *Analityk informacji w administracji rządowej* [w:] *Analiza informacji w zarządzaniu bezpieczeństwem. Zarządzaniem bezpieczeństwem*, *(red.) K. Liedel, P. Piasecka, T.R. Aleksandrowicz*, Warszawa, Wyd. Difin SA, 2013.

Błażewski M., **Behr J.**, *Środki prawne ochrony danych osobowych*, Wrocław, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2018.

Gumularz M., **Kozik P.**, *Ochrona danych osobowych. Kontrola i postępowanie w sprawie naruszenia przepisów. Poradnik ze wzorami*, Wydanie 2, Warszawa, Wolters Kluwer, 2022.

Instrukcja podstawowych zasad bezpieczeństwa dla pracowników KRUS, Wydanie XVII, 28 października 2024.

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. nr 78 poz. 483 ze zm.

KRUS, *Przetwarzanie danych osobowych*, https://www.gov.pl/web/krus/przetwarzanie-danych-osobowych--rodo, dostęp 26.04.2022.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa, C.H. Beck, 2016.

Księga Zintegrowanego Systemu Zarządzania KRUS, Wydanie XXIII, 1 października 2024.

Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydanie II, Warszawa, PWN, 2017.

Oleksiewicz I., **Krztoń W.**, *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Warszawa, Rambler Press, 2017.

Oświadczenie Przewodniczącej Europejskiej Rady Ochrony Danych Andrea Jelinek w sprawie przetwarzania danych osobowych w kontekście pandemii COVID-19 z 19 marca 2020 roku.

Sobczak A., *RODO Rozproszona władza publiczna*, Wydanie I, Kraków, Wyd. Uniwersytetu Jagiellońskiego, 2019.

UODO, https://uodo.gov.pl/pl/138/1459, dostęp 26.04.2022.

UODO, https://uodo.gov.pl/pl/126/208, dostęp 7.02.2025.

Ustawa z 6 września 2001 r. o dostępie do informacji publicznej, Dz. U. 2022 poz. 902.

Ustawa z 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2019 poz. 1781.

Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. 2024 poz. 632 ze zm.

Ustawa z 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników, Dz. U. 2024 poz. 90 ze zm.

Wojciechowska-Filipek S., **Ciekanowski Z.**, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki-Organizacji-Państwa*, Wydanie II, Warszawa, CeDeWu, 2019.

Wójcik G.P., *Obowiązki przedsiębiorców wynikające z RODO*, Wydanie I, Warszawa, CeDeWu, 2021.

Zarządzenie Nr 15 Prezesa Kasy rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r. w sprawie wprowadzenia w Kasie Rolniczego Ubezpieczenia Społecznego Polityki bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, Dz. Urz. KRUS 2024 poz. 16.

otrzymano: 10.02.2025
zaakceptowano: 18.04.2025