B&W BRUDKOWSKI & WSPÓLNICY

NEWSLETTER Nr 7

Szanowni Państwo,

Zapraszamy do lektury kolejnego wydania naszego Newslettera.

Spis treści

1. PRAWO KOMUNIKACJI ELEKTRONICZNEJ 2
2. USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA 3
3. USTAWA O OCHRONIE SYGNALISTÓW 5
4. NAJNOWSZE AKTY WYKONAWCZE DO DORA 6
5. PRAWO BANKOWE 9
6. ROZPORZĄDZENIE W SPRAWIE MEDYCZNYCH LABORATORIÓW DIAGNOSTYCZNYCH 10
7. ZMIANA TERMINU NA WDROŻENIE E-DELIVERY 11

I. PRAWO KOMUNIKACJI ELEKTRONICZNEJ

- √ 9 sierpnia 2024 r., prezydent RP podpisał ustawę Prawo Komunikacji Elektronicznej, które zastąpi dotychczas obowiązujące Prawo Telekomunikacyjne.
- √ Prawo Komunikacji Elektronicznej wdraża unijną dyrektywę 2018/1972 ustanawiającą Europejski kodeks łączności elektronicznej oraz dyrektywę 2022/2380.
- √ Nowa ustawa wprowadza istotne zmiany i nakłada kolejne obowiązki na przedsiębiorców komunikacji elektronicznej obejmując nowy krąg podmiotów niepodlegających wcześniejszej regulacji.

Główny cel: ujednolicenie regulacji i zwiększenie spójności rynku telekomunikacyjnego w Unii Europejskiej.

Kogo chronią zmiany: Przepisy nowej ustawy poświęcone są ochronie interesów konsumentów, m.in. poprzez obowiązki nałożone na przedsiębiorców w postaci przejrzystości porównywania ofert czy obligatoryjnego podsumowania warunków umowy.

Nowość: obok usług telekomunikacyjnych, dostarczania sieci telekomunikacyjnych i świadczenia usług z tym powiązanych ustawa tworzy kategorię podmiotów kwalifikowanych jako przedsiębiorcy komunikacji elektronicznej, czyli przedsiębiorcy telekomunikacyjni lub podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów (np. Messenger), a więc świadczonych głównie za pośrednictwem Internetu.

Obowiązki nałożone na przedsiębiorców:

- doręczenie konsumentowi informacji przedumownych oraz zwięzłe podsumowanie warunków umowy,
- zakaz dyskryminacji użytkowników ze względu na obywatelstwo, miejsce zamieszkania lub siedzibę,
- publikowanie na stronie internetowej informacji o oferowanych usługach, ich cechach oraz cenach,
- ograniczenia dotyczące jednostronnej zmiany warunków umowy przez dostawcę usług,
- zapewnienie użytkownikom z niepełnosprawnościami dostępu do usług w sposób równoważny do dostępu, z jakiego korzysta większość użytkowników.

Ważne:

- √ Przedsiębiorcy będą zobowiązani do zachowania tajemnicy komunikacji elektronicznej oraz do zabezpieczania urządzeń telekomunikacyjnych, publicznych sieci telekomunikacyjnych oraz danych przed ujawnieniem tajemnicy.

√ Dostawcy usług komunikacji elektronicznej będą musieli informować użytkowników końcowych o zakresie i celu przetwarzania danych oraz o możliwościach wpływu na ten proces.

√ W przypadku niewykonania lub nienależytego wykonania obowiązków, Prezes Urzędu Komunikacji Elektronicznej będzie mógł nałożyć na przedsiębiorców komunikacji elektronicznej karę pieniężną do 3% przychodu osiągniętego w poprzednim roku kalendarzowym.

***Użytkownik końcowy** – zgodnie z definicją ustawową jest to podmiot korzystający z publicznie dostępnej usługi komunikacji elektronicznej lub żądający świadczenia takiej usługi, dla zaspokojenia własnych potrzeb.

Kluczowe założenia:

- ujednolicenie ładowarek do telefonów i innych urządzeń mobilnych,
- dostarczenie konsumentowi bezpłatnie na trwałym nośniku zwięzłego podsumowania warunków umowy,
- ustawa uniemożliwia związanie konsumenta z danym dostawcą na okres dłuższy niż 24 miesiące i pozwala na częstsze niż dotychczas korzystanie z różnorodności wyboru usługi i dostawcy,
- dostawca jest zobowiązany zwrócić konsumentowi środki z doładowań pozostałe na koncie,
- powstanie narzędzie do porównywania dostępnych na rynku ofert usług dostępu do Internetu oraz usług komunikacji interpersonalnej - narzędzie będzie certyfikowane przez Prezesa Urzędu Komunikacji Elektronicznej na wniosek podmiotu oferującego to narzędzie, a informacja o gotowości jego powstania pojawi się w Biuletynie Informacji Publicznej Urzędu Komunikacji Elektronicznej.
    - Użytkownicy końcowi będą dzięki temu mieć bezpłatny dostęp do porównania ofert w przejrzysty sposób, informacje zawarte w narzędziu mają być jednoznaczne, aktualne i otwarte dla każdego dostawcy usług (por. art. 313 ust. 1 Ustawy)
- zgody na komunikację marketingową zostaną zredukowane.

II. USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

√ Ministerstwo Cyfryzacji zbliża się do zakończenia prac nad nowelizacją przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa *nota bene* wdrażającej dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej.

√ **Główny cel:** Wdrożenie unijnych przepisów – Toolbox 5G oraz dyrektywy NIS 2.

√ **Czas na wdrożenie:** 17 października 2024 roku.

Toolbox 5G główne założenia:

- harmonizacja i standaryzacja sieci 5G na poziomie unijnym,
- 3 rodzaje środków zabezpieczających – na poziomie strategicznym (dot. większych uprawnień dla organów właściwych), wspierającym (dot. prac nad europejskim programem standaryzacji) oraz technicznym (dot. badania bezpieczeństwa oprogramowania).

Dyrektywa NIS 2 główne założenia:

- nałożenie na kluczowe i ważne podmioty nowych obowiązków dotyczących zapewnienia bezpieczeństwa cybernetycznego,
- instytucje będą zobowiązane wdrożyć system zarządzania bezpieczeństwem informacji w ramach procesów związanych z świadczeniem usług.
    - **system taki powinien gwarantować m.in.:**
        - √ prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
        - √ wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy;
        - √ zbieranie informacji o zagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;
        - √ zarządzanie incydentami;
        - √ stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi;

Kto będzie podmiotem kluczowym?

- Osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, wskazana w załącznikach do ustawy (dostawcy energii, żywności, chemikaliów etc.), która przewyższa wymogi dla średniego przedsiębiorstwa,
- Przedsiębiorca komunikacji elektronicznej,
- Niezależnie od wielkości podmiotu: podmiot krytyczny, podmiot publiczny, dostawca usług DNS.

***podmiot krytyczny** - Dyrektywa NIS2 definiuje w ten sposób sektor administracji publicznej

***dostawcy usług DNS** – Dyrektywa definiuje dostawców jako osoby prawne świadczące usługi cyfrowe, tj. usługi, które są świadczone za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usługi. W rozumieniu polskiej ustawy o krajowym systemie cyberbezpieczeństwa, implementującej dyrektywę NIS, do usług cyfrowych zaliczamy: internetową platformą handlową, wyszukiwarkę internetową lub usługę przetwarzania w chmurze.

Kto będzie podmiotem ważnym?

- Osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, wskazana w załącznikach do ustawy, która nie jest podmiotem kluczowym,
- Niekwalifikowani dostawcy usług zaufania będący mikro-, małymi lub średnimi przedsiębiorcami;
- Przedsiębiorcy komunikacji elektronicznej będący mikro-, lub małymi przedsiębiorcami w rozumieniu rozporządzenia;
- Podmioty zidentyfikowane jako podmioty ważne przez organ właściwy do spraw cyberbezpieczeństwa.

√ **dyrektywa NIS 2 zakłada samoidentyfikację podmiotów, które zobowiązane są następnie złożyć wniosek o wpis do wykazu podmiotów kluczowych i ważnych.** Nowe przepisy umożliwiają jednak wpisanie określonego podmiotu do wykazu, jeżeli nie złożył on wniosku o wpis, a spełnia przesłanki uznania go za kluczowy lub ważny.

III. USTAWA O OCHRONIE SYGNALISTÓW

√ Wielkimi krokami zbliża się termin wejścia w życie długo oczekiwanej ustawy o ochronie sygnalistów,

√ Nowa ustawa zacznie obowiązywać 25 września 2024 r.

√ Pracodawcy muszą się przygotować nie tylko na wdrożenie samych procedur zgłaszania nieprawidłowości, ale też zastanowić się, w jaki sposób szeroko zakrojona ochrona sygnalistów będzie wpływała na bieżące zarządzanie procesami HR w ich organizacjach i jak uchronić się przed podejrzeniami o stosowanie działań odwetowych.

Absolutny zakaz działań odwetowych

Przepisy ustawy zakazują pracodawcom działań odwetowych wobec sygnalisty. Pracodawca nie może stosować jakichkolwiek represji wobec sygnalisty z powodu dokonania zgłoszenia lub ujawnienia publicznego. Ustawa zawiera otwarty katalog działań odwetowych. Tytułem przykładu:

- nieprzyznanie sygnaliście premii albo nagrody,
- pominięcie sygnalisty w procedurze awansu,
- przekazanie obowiązków sygnalisty innemu pracownikowi,
- niekorzystna zmiana rozkładu czasu pracy sygnalisty,
- wyrażenie „negatywnej opinii" o pracy sygnalisty.

Ważne: Zgodnie z art. 55 ustawy – podejmowanie działań odwetowych wobec sygnalisty obwarowane będzie sankcjami karnymi w postaci grzywny, kary ograniczenia wolności, a nawet – pozbawienia wolności do 2 lat.

Ustawa wprowadza zasadę, że to na pracodawcy spoczywać będzie ciężar dowodu, że podjęte wobec sygnalisty działanie nie jest działaniem odwetowym. To nie pracownik będzie musiał wykazać, że pracodawca w jakiś sposób „zemścił się" na nim za dokonane zgłoszenie, lecz odwrotnie – pracodawca zmuszony będzie do udowodnienia, że tak nie było.

Biorąc jednak pod uwagę wspomniane przepisy ochronne, pracodawca powinien dołożyć starań, by dysponować materiałem dowodowym, który – w razie postawienia takiego zarzutu przez pracownika sygnalistę – pozwoli stwierdzić, że działanie nie miało nic wspólnego z odwetem na sygnaliście.

IV. NAJNOWSZE AKTY WYKONAWCZE DO DORA

√ Najnowsze akty wykonawcze do DORA zostały opublikowane przez Europejskie Urzędy Nadzoru do Komisji Europejskiej 17 lipca 2024 r., trafiły teraz do Komisji Europejskiej, która może wprowadzić dodatkowe zmiany.

√ **do kogo skierowane jest rozporządzenie:** do podmiotów finansowych, w szczególności do: instytucji kredytowych, instytucji płatniczych, instytucji pieniądza elektronicznego,

firm inwestycyjnych, dostawców usług w zakresie kryptoaktywów, emitentów kryptoaktywów, dostawców usług w zakresie udostępniania informacji, zakładów ubezpieczeń i zakładów reasekuracji, pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające, instytucji pracowniczych programów emerytalnych, agencji ratingowych, biegłych rewidentów i firm audytorskich, administratorów kluczowych wskaźników referencyjnych, dostawców usług finansowania społecznościowego, repozytoriów sekurytyzacji, zewnętrznych dostawców usług ICT.

√ **czas na wdrożenie:** Podmioty wskazane powyżej mają czas na wdrożenie rozporządzenia DORA do 17 stycznia 2025 r.

√ Opublikowane w lipcu akty wykonawcze do rozporządzenia DORA (tzw. RTS) przewidują konieczność składania aż **trzech różnych raportów** związanych z poważnym incydentem ICT (teleinformatycznym)

- DORA wskazuje, że z **poważnym incydentem ICT** mamy do czynienia, jeśli ma on duży negatywny wpływ na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego.

- **Raporty:** w każdym z nich należy opisać jak najbardziej aktualną sytuację. W każdym ze sprawozdań są też wskazane do opisania konkretne punkty. W przypadku **raportu wstępnego** jest siedem punktów obowiązkowych oraz trzy dodatkowe. W trakcie konsultacji projektu RTS zmniejszono, pod naciskiem rynku, liczbę tych pytań. **W sprawozdaniu pośrednim** organizacja musi odpowiedzieć aż na 14 pytań obowiązkowych i 21 dodatkowych. **W sprawozdaniu końcowym** należy opisać siedem kwestii obowiązkowo i siedem dodatkowych. Oznacza to, że we wszystkich trzech raportach podmiot finansowy będzie musiał wypełnić aż 28 obowiązkowych rubryk i 31 dodatkowych. Skala raportowania jest więc bardzo duża, na co w trakcie konsultacji zwracali uwagę przedstawiciele rynku finansowego z całej Europy.

- DORA wymaga raportowania poważnych incydentów do odpowiednich organów nadzorczych w ciągu 4 godzin od zakwalifikowania incydentu jako poważnego, jednak nie później niż w ciągu 24 godzin od momentu, gdy podmiot dowiedział się o zdarzeniu. Jest to termin dla raportu wstępnego. Po nim należy jeszcze złożyć raport śródokresowy (w ciągu 72 godzin) oraz końcowy (w ciągu miesiąca). Dlatego tak ważne jest opracowanie odpowiednich systemów monitorowa-

-nia które będą obejmować opracowanie procedur eskalacji incydentów, jak również zapewnienie, że pracownicy są odpowiednio przeszkoleni w zakresie zgłaszania incydentów.

- Ostatecznie w RTS-ach przewidziano sytuację, w której organizacja nie będzie w stanie złożyć kompletnego powiadomienia wstępnego lub któregoś ze sprawozdań (pośredniego lub końcowego). W takiej sytuacji podmiot finansowy powinien powiadomić organ o tym, że takiego raportu w terminie jest w stanie złożyć. Powinien to zrobić bez zbędnej zwłoki, jednak nie później niż w odpowiednim terminie złożenia powiadomienia/sprawozdania. Należy też wyjaśnić przyczyny opóźnienia.

√ **Obowiązek nałożony na podmioty finansowe**: poinformowanie swoich klientów o zaistniałych incydentach. Dotyczy to poważnych incydentów związanych z ICT, które mają istotny wpływ na interesy finansowe klientów. W takim przypadku podmioty finansowe powinny przekazywać swoim klientom informacje o incydentach niezwłocznie po tym, gdy dowiedzą się o ich wystąpieniu. W informacji tej powinny znaleźć się środki, które podjęto, aby złagodzić negatywne skutki incydentu

Ważne:

- **Banki i instytucje kredytowe** muszą spełniać wysokie standardy zarządzania ryzykiem ICT oraz raportowania incydentów. Obejmuje to również wymagania dotyczące testowania systemów oraz utrzymania planów BCP (z ang. Business Continuity Planning – Plan Ciągłości Działania). BCP powinien obejmować scenariusze awaryjne, procedury odzyskiwania danych oraz testy scenariuszowe, które symulują różne rodzaje ataków cybernetycznych.

- **Firmy ubezpieczeniowe** podobnie jak banki, muszą wdrożyć solidne mechanizmy zarządzania ryzykiem ICT. Obejmuje to nie tylko ocenę wewnętrznych systemów IT, ale także całego łańcucha dostaw ICT, w tym dostawców usług zewnętrznych. Przykłady praktyczne mogą obejmować audyty bezpieczeństwa IT, oceny ryzyka na poziomie zarządu oraz weryfikację polityk bezpieczeństwa. Dodatkowo, muszą monitorować zagrożenia związane z polisami cybernetycznymi i uwzględniać je w swoich strategiach zarządzania ryzykiem.

- **Dostawcy usług płatniczych** muszą zapewnić, że ich systemy są odporne na ataki cybernetyczne, a także że transakcje płatnicze są bezpieczne i niezawodne. Wymaga to ścisłego monitorowania oraz regularnego testowania systemów.

- **Dostawcy usług ICT** muszą spełniać określone standardy bezpieczeństwa, a także współpracować z instytucjami finansowymi w zakresie zarządzania ryzykiem i reagowania na incydenty. Obejmuje to również wymagania dotyczące audytów i certyfikacji bezpieczeństwa.

V. PRAWO BANKOWE

√ wraz z nadchodzącym wrześniem 2024 roku w życie wchodzą nowe regulacje dotyczące korzystania z produktów bankowych.

√ **cel zmian**: poprawa bezpieczeństwa klientów, zwiększenie przejrzystości usług oraz dostosowanie się do nowych unijnych dyrektyw. Wrześniowe zmiany w przepisach dotyczących produktów bankowych to krok w stronę większej przejrzystości i bezpieczeństwa dla klientów.

Istotne zmiany:

- **Nowe Wytyczne Dotyczące Kredytów Konsumenckich -** Banki będą zobowiązane do udzielania jasnych i zrozumiałych informacji, które pomogą klientom w podjęciu świadomej decyzji.

- **Obowiązkowa Analiza Zdolności Kredytowej -** Banki będą musiały jeszcze dokładniej analizować zdolność kredytową klientów. Wprowadzenie nowych kryteriów oceny ma na celu zmniejszenie ryzyka udzielania kredytów osobom, które mogą mieć trudności z ich spłatą,

- **Nowe Limity Opłat i Prowizji -** od września obowiązywać będą nowe limity dotyczące opłat i prowizji za udzielenie kredytów konsumenckich. Ograniczenia te mają na celu ochronę konsumentów przed nadmiernymi kosztami związanymi z zaciągnięciem zobowiązań finansowych.

- **Nowe Wymogi Dotyczące Ubezpieczeń Bankowych -** Banki będą musiały dostosować się do nowych przepisów dotyczących oferowania ubezpieczeń, które są sprzedawane razem z produktami bankowymi, takimi jak kredyty hipoteczne czy konta oszczędnościowe

VI. ROZPORZĄDZENIE W SPRAWIE MEDYCZNYCH LABORATORIÓW DIAGNOSTYCZNYCH

√ W Dzienniku Ustaw (Dz. U. 2024 poz. 1188) opublikowano rozporządzenie ministra zdrowia dotyczące wymagań medycznych laboratoriów diagnostycznych oraz kwalifikacji personelu.

√ Rozporządzenie dotyczy podmiotów leczniczych, a także podmiotów, które nie udzielają świadczeń zdrowotnych, jednakże posiadają laboratorium (uczelnia, instytut badawczy niebędący podmiotem leczniczym)

√ Przepisy weszły w życie 7 sierpnia 2024 r.

Kluczowe założenie: pomieszczenia laboratorium powinny być dostosowane do rodzaju prac, jakie są w nich wykonywane, w sposób zapewniający poprawną jakość pomiarów i wiarygodność wyników. Wymieniono także rodzaje pomieszczeń, które wchodzą w skład laboratorium z podziałem na pomieszczenie główne, socjalne, specjalne, pomieszczenie służące do obsługi pacjentów oraz administracyjne.

Nowości:

- dostosowano stanowiska i kwalifikacje do przepisów rozporządzenia Ministra Zdrowia z dnia 10 lipca 2023 r. w sprawie kwalifikacji wymaganych od pracowników na poszczególnych rodzajach stanowisk pracy **w podmiotach leczniczych niebędących przedsiębiorcami**, z wyjątkiem stanowisk niemających zastosowania w laboratoriach diagnostycznych np. starsza salowa/ sanitariusz, salowa/ sanitariusz,

  √ **katalog podmiotów leczniczych niebędących przedsiębiorcami określa ustawa z dnia 15.04.2011 r. o działalności leczniczej. Są to podmioty lecznicze wymienione w art. 4 ust. 1 pkt 2, 3 i 7 ww. Ustawy, a zatem:**

  - samodzielne publiczne zakłady opieki zdrowotnej,
  - jednostki budżetowe, w tym państwowe jednostki budżetowe tworzone i nadzorowane przez Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Ministra Sprawiedliwości lub Szefa Agencji Bezpieczeństwa Wewnętrznego, posiadające w strukturze organizacyjnej ambulatorium, ambulatorium z izbą chorych lub lekarza podstawowej opieki zdrowotnej, pielęgniarkę podstawowej opieki zdrowotnej lub położną podstawowej opieki zdrowotnej w rozumieniu przepisów ustawy z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz. U. z 2022 r. poz. 2527),

- jednostki wojskowe w zakresie, w jakim wykonują działalność leczniczą.

- **Ważne**: zgodne z § 9 Rozporządzenia - Podmiot wykonujący działalność leczniczą w zakresie medycyny laboratoryjnej, uczelnia oraz instytut badawczy niebędący podmiotem leczniczym, które prowadzą laboratorium, dostosują swoją działalność do wymagań w zakresie kwalifikacji na poszczególnych stanowiskach określonych w załączniku do rozporządzenia w terminie 4 lat od dnia wejścia w życie niniejszego rozporządzenia.

- w załączniku do Rozporządzenia w wykazie kwalifikacji personelu i kierownika laboratorium dodano stanowiska pracy dla starszego technologa laboratoryjnego, technologa laboratoryjnego oraz młodszego technologa laboratoryjnego ze wskazaniem wymaganych kwalifikacji zawodowych.

- z uwagi na funkcjonowanie wielospecjalistycznych laboratoriów diagnostycznych utworzono nowe stanowisko kierownika pracowni,

- określono wymagania dla kierownika laboratorium w zakresie kwalifikacji zawodowych zgodnie z przepisami ustawy z dnia 15 września 2022 r. o medycynie laboratoryjnej,

- w zakresie stanowisk starszy laborant medycyny laboratoryjnej i laborant medycyny laboratoryjnej wskazano, iż na tych stanowiskach mogą być zatrudnione osoby, które w dniu wejścia w życie rozporządzenia posiadały kwalifikacje do wykonywania czynności medycyny laboratoryjnej w rozumieniu dotychczasowych przepisów i były zatrudnione w laboratorium.

Uwaga: Ujęto także przepis przejściowy, zgodnie z którym uczelnia albo instytut badawczy (niebędące podmiotem leczniczym), które prowadzą laboratorium, dostosują pomieszczenia laboratoriów do wymagań określonych w niniejszym rozporządzeniu w terminie 6 miesięcy od dnia wejścia w życie niniejszego rozporządzenia.

VII. ZMIANA TERMINU NA WDROŻENIE E-DELIVERY

√ Minister Cyfryzacji zmienił termin obowiązku stosowania e-Doręczeń przez podmioty wskazane w ustawie o doręczeniach elektronicznych. Pozwoli to na przeprowadzenie nowelizacji ustawy o doręczeniach oraz innych ustaw, wprowadzając okres przejściowy w stosowaniu e-Doręczeń.

√ Obowiązek wchodzi w życie 1 stycznia 2025 r., a nie 1 października 2024 r.

Zgodnie z wcześniejszymi zapowiedziami Ministerstwa, kontynuowane będą działania informacyjno-wdrożeniowe skierowane do podmiotów publicznych, działania mające na celu wdrożenie systemów klasy EZD (Elektroniczne Zarządzanie Dokumentacją) w podmiotach publicznych oraz zmiany w systemie e-Doręczeń, dostosowujące go w większym stopniu do potrzeb użytkowników.

Ważne: Skuteczne wprowadzenie e-Doręczeń w podmiotach publicznych wymaga wprowadzenia okresu przejściowego — do 31 grudnia 2025 r., w którym będą one mogły stopniowo dostosowywać się do nowego sposobu prowadzenia korespondencji. W okresie tym zostanie zapewniona równoważność doręczenia za pośrednictwem operatora pocztowego albo w ePUAP oraz innych systemach dziedzinowych z e-Doręczeniami. Przy czym wprowadzane rozwiązania legislacyjne będą promować doręczanie korespondencji z wykorzystaniem e-Doręczeń.

Wdrożenie nowego rozwiązania na tak dużą skalę – wszystkie podmioty publiczne, zawody zaufania publicznego, przedsiębiorcy wpisani do CEIDG oraz podmioty wpisane do KRS – jest procesem, który musi następować stopniowo i odbywać się równolegle z działaniami informacyjnymi (tj. upowszechnienie podstawowej wiedzy nt. nowego rozwiązania) oraz działaniami promocyjnymi (przedstawienie korzyści z nowego rozwiązania).