PORADNIK

System MDM w jednostkach samorządu terytorialnego

Obowiązki prawne, model wdrożenia i kryteria zakupu

CyberKatalog.pl

Wydanie drugie | Wrzesień 2026
Stan prawny na 19 września 2026 r.

Wydawca: CyberKatalog.pl
Wydanie: drugie, wrzesień 2026
Stan prawny: 19 września 2026 r.
Format: Publikacja elektroniczna
Zdjęcie na okładce: Malwina Nogaj, Unsplash (licencja Unsplash)

O publikacji

Poradnik jest przeznaczony dla osób, które w jednostce samorządu terytorialnego odpowiadają za bezpieczeństwo informacji, informatykę, ochronę danych osobowych albo za zakupy: sekretarzy, informatyków, inspektorów ochrony danych, pełnomocników do spraw cyberbezpieczeństwa i osób przygotowujących zamówienia. Opisuje, czego prawo wymaga od urzędu w odniesieniu do służbowych urządzeń mobilnych, jak te wymagania przekładają się na funkcje systemu zarządzania urządzeniami mobilnymi (MDM) i jak opisać taki system w zamówieniu publicznym.

Metoda

Każde twierdzenie o obowiązku prawnym wskazuje akt i jednostkę redakcyjną, z której wynika. Treść przepisów odczytano bezpośrednio z tekstów ogłoszonych w dziennikach urzędowych: Dzienniku Ustaw, Monitorze Polskim, dzienniku urzędowym ministra i Dzienniku Urzędowym Unii Europejskiej. Zalecenia techniczne opierają się na publikacji amerykańskiego National Institute of Standards and Technology (NIST SP 800-124 Rev. 2), instytucji publicznej niezależnej od producentów. Poradnik nie cytuje materiałów producentów systemów MDM ani forów internetowych i nie wymienia z nazwy żadnego produktu MDM.

Stan prawny

Poradnik uwzględnia stan prawny na 19 września 2026 r. W szczególności obejmuje nowelizację ustawy o krajowym systemie cyberbezpieczeństwa z 23 stycznia 2026 r., która weszła w życie 3 kwietnia 2026 r., oraz rozporządzenie w sprawie Krajowych Ram Interoperacyjności z 21 maja 2024 r., które traci moc z dniem 23 lutego 2027 r. (art. 1 pkt 19 w zw. z art. 17 ustawy z 25 lipca 2025 r.). Terminy, które upływają po dniu wydania, opisano według brzmienia przepisów w tym dniu.

Zastrzeżenie

Poradnik nie jest opinią prawną. Kwalifikacja konkretnej jednostki jako podmiotu kluczowego albo ważnego, zakres jej obowiązków i treść dokumentacji zamówienia wymagają oceny w okolicznościach tej jednostki.

Spis treści

Spis rysunków

Spis tabel

Rozdział 1

Urządzenia mobilne w urzędzie

1.1 Skala zjawiska

Według Głównego Urzędu Statystycznego w 2025 r. 90,0% jednostek administracji samorządowej wyposażało pracowników w urządzenia przenośne z mobilnym dostępem do internetu, a takie urządzenie miało 23,4% pracowników administracji samorządowej. W administracji rządowej odsetki wynosiły odpowiednio 99,1% jednostek i 51,8% pracowników [1].

Oba wskaźniki mówią coś innego. Pierwszy pokazuje, że służbowe urządzenie mobilne jest w samorządzie standardem. Drugi pokazuje, że w administracji samorządowej ma je mniej niż co czwarty pracownik. Badanie nie wskazuje, na jakich stanowiskach. Nie mierzy też, ile z tych urządzeń jest objętych centralnym zarządzaniem ani ile urzędów pozwala pracownikom korzystać z poczty służbowej na telefonie prywatnym.

1.2 Co może się stać z urządzeniem

Publikacja NIST SP 800-124 Rev. 2, wydana przez amerykański National Institute of Standards and Technology w maju 2023 r., jest opracowaniem instytucji publicznej niezależnej od producentów, poświęconym zarządzaniu bezpieczeństwem urządzeń mobilnych w organizacji [2]. W rozdziale 3 wymienia trzynaście zagrożeń dotyczących samych urządzeń i cztery dotyczące platformy, która nimi zarządza. Dla urzędu najważniejsze są te, które nie wymagają zaawansowanego przeciwnika:

- utrata lub kradzież urządzenia (3.1.2), która przy braku blokady ekranu i szyfrowania oznacza ujawnienie wszystkiego, co jest w pamięci i w zalogowanych aplikacjach;
- wykorzystanie znanych podatności systemu operacyjnego (3.1.1), bo urządzenie bez aktualizacji albo model, którego producent przestał wspierać, pozostaje podatne na błędy opisane publicznie;
- dostęp do zasobów organizacji z urządzenia źle skonfigurowanego (3.1.4) i z urządzenia niezaufanego (3.1.7);
- kradzież danych logowania przez phishing, także przez wiadomości SMS i komunikatory (3.1.5);

- utrata danych przez synchronizację z prywatną chmurą użytkownika (3.1.12) i korzystanie z usług, których organizacja nie zatwierdziła (3.1.13);
- naruszenie prywatności użytkownika przez samą organizację (3.1.11), co w polskim porządku prawnym ma wymiar prawa pracy i RODO.

Zagrożenia z części 3.2.1-3.2.4 dotyczą samego systemu MDM. Według NIST przejęcie danych logowania administratora pozwala zmienić polityki tak, by urządzenia straciły zabezpieczenia, albo odebrać dostęp do zasobów organizacji wszystkim urządzeniom naraz (3.2.2), a sama platforma działa na typowym sprzęcie i oprogramowaniu, które trzeba konfigurować i aktualizować jak każdy system (3.2.1). Wdrożenie MDM przesuwa więc część ryzyka z urządzeń na konsolę i wymaga jej ochrony, o czym jest mowa w rozdziale 7.

1.3 Czym jest zarządzanie, a czym nie jest

Zarządzanie urządzeniem mobilnym nie polega na obserwowaniu pracownika. Polega na tym, że urząd wie, jakie urządzenia mają dostęp do jego danych, w jakim są stanie i co może z nimi zrobić, gdy coś pójdzie źle. Sześć rekomendacji otwierających publikację NIST obejmuje analizę zagrożeń dla urządzeń mobilnych i systemów z nich dostępnych, zastosowanie technologii bezpieczeństwa mobilnego, pilotaż przed wdrożeniem produkcyjnym, pełne zabezpieczenie każdego urządzenia wydanego przez organizację przed dopuszczeniem go do jej systemów, aktualność systemów i aplikacji oraz regularne monitorowanie i utrzymywanie bezpieczeństwa urządzeń [2]. Tylko jedna z nich dotyczy wyboru narzędzia; pozostałe opisują proces, bez którego narzędzie niczego nie zabezpiecza.

Kolejność rozdziałów poradnika wynika z tej samej logiki. Rozdział 2 porządkuje pojęcia, rozdział 3 ustala, czego wymaga prawo, rozdziały 4 i 5 opisują cykl życia urządzenia i zasady, które urząd musi przyjąć, a dopiero rozdział 6 dotyczy wyboru systemu.

Materiały pokrewne

Definicje pojęć MDM, EMM, UEM i BYOD wraz z diagramami zawiera hasło słownika CyberKatalog.pl poświęcone systemom MDM [3]. Obowiązki samorządów po nowelizacji KSC w krótszej formie omawia artykuł Silesian Solutions o MDM w jednostkach samorządu terytorialnego [4].

Rozdział 2

Pojęcia i modele

2.1 MDM, MAM, EMM i UEM

Nazwy kategorii oprogramowania do zarządzania urządzeniami nie mają jednej, powszechnie przyjętej definicji. Poradnik stosuje definicje z publikacji NIST SP 800-124 Rev. 2 [2], bo jest to opracowanie instytucji publicznej, niezależne od producentów.

MDM (*mobile device management*, zarządzanie urządzeniami mobilnymi): zarządzanie całym urządzeniem zarejestrowanym w organizacji: konfiguracją, ustawieniami bezpieczeństwa, aplikacjami i zdalnymi poleceniami, takimi jak blokada i wymazanie. Wymaga, by właściciel urządzenia zgodził się na jego rejestrację i instalację profilu zarządzania (4.2.2) [3].

MAM (*mobile application management*, zarządzanie aplikacjami mobilnymi): zarządzanie wybranymi aplikacjami i danymi w nich, bez przejmowania kontroli nad urządzeniem. Według NIST systemy MAM nie wymagają rejestracji urządzenia ani instalacji profilu organizacji, a przy urządzeniach prywatnych zastosowanie MAM zamiast MDM może ograniczyć obawy użytkowników o prywatność (4.2.2) [5].

EMM (*enterprise mobility management*, zarządzanie mobilnością w przedsiębiorstwie): rozwiązanie do wdrażania, konfigurowania i aktywnego zarządzania urządzeniami mobilnymi, które może obejmować MDM, MAM, ochronę przed zagrożeniami mobilnymi i inne technologie (4.2.1) [6].

UEM (*unified endpoint management*, ujednolicone zarządzanie punktami końcowymi): NIST traktuje tę nazwę jako inne określenie EMM (4.2.1). Nazwa bywa też używana szerzej, dla rozwiązań obejmujących również komputery. Hasło UEM w słowniku CyberKatalog.pl opisuje to rozróżnienie [7].

Dla urzędu z tych rozróżnień wynika jedno praktyczne pytanie: czy system ma zarządzać całym urządzeniem, czy tylko danymi służbowymi na nim. Odpowiedź zależy od modelu własności. Nazwa kategorii, pod którą produkt jest sprzedawany, jej nie rozstrzyga. Dlatego rozdział 6 proponuje opisywać przedmiot zamówienia funkcjami.

2.2 Jak system zarządza urządzeniem

Urządzenie nie daje się zarządzać dowolnemu programowi. Główne platformy mobilne udostępniają interfejsy zarządzania, które pozwalają konfigurować ustawienia bezpieczeństwa, sterować aplikacjami i odczytywać informacje o urządzeniu, a dostęp do tych interfejsów musi zaakceptować użytkownik urządzenia albo dział IT organizacji. Większość platform pozwala, by urządzeniem sterował tylko jeden system MDM. Polecenia administratora mogą trafiać do urządzenia bezpośrednio albo przez infrastrukturę właściciela platformy (rysunek 2.1), który przekazuje je dalej (NIST SP 800-124 Rev. 2, 4.1.3) [2].

Rysunek 2.1: Elementy systemu MDM w wariancie, w którym polecenia trafiają do urządzenia przez infrastrukturę właściciela platformy. Katalog tożsamości, rejestr zdarzeń i zasoby urzędu istnieją niezależnie od MDM; system jest z nimi integrowany.

Z tej konstrukcji wynikają trzy konsekwencje dla urzędu. Po pierwsze, system MDM zależy od usług twórców systemów operacyjnych: konto urzędu w ich programach dla organizacji jest częścią wdrożenia i musi mieć właściciela w urzędzie, a nie wyłącznie u wykonawcy. Po drugie, zakres tego, co administrator może zrobić z urządzeniem, wyznacza platforma i sposób rejestracji, a nie sam system MDM. Po trzecie, zmiana systemu MDM oznacza zwykle ponowną rejestrację wszystkich urządzeń.

2.3 Modele własności urządzeń

NIST opisuje trzy najczęściej stosowane kategorie modeli wdrożenia (5.1.3) [2]:

Użytek wyłącznie służbowy (*Strict Enterprise Usage*): urządzenie wydane i posiadane przez organizację, przeznaczone wyłącznie do celów służbowych; użytkownicy wiedzą, że wszystkie dane na nim kontroluje organizacja. Model ten bywa określany skrótem COBO (*corporate-owned, business-only*), którego NIST nie używa.

COPE (*corporate-owned, personally enabled*): urządzenie organizacji z dopuszczonym ograniczonym użytkiem prywatnym. Urządzenie i informacje na nim należą do organizacji [8].

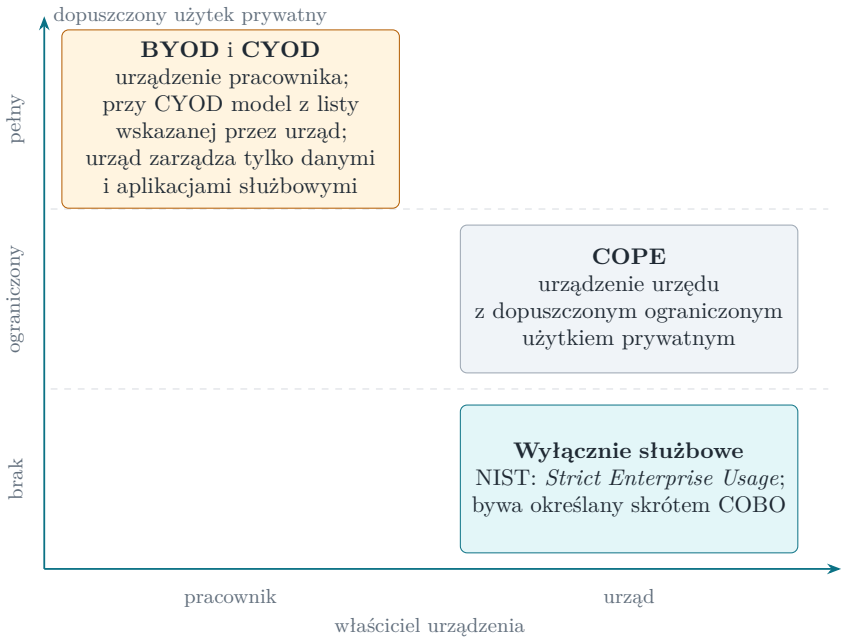
BYOD i CYOD (*bring your own device*, *choose your own device*): urządzenia należące do pracownika. W modelu CYOD pracownik kupuje urządzenie do własnego użytku,

ale wybiera je z listy modeli wskazanych przez organizację, zdolnych do uruchomienia wymaganego oprogramowania zabezpieczającego. Model BYOD i jego ryzyka opisuje też słownik CyberKatalog.pl [9].

Skróty te bywają używane niejednolicie, zwłaszcza CYOD: hasło w słowniku CyberKatalog.pl dopuszcza przy CYOD także urządzenie należące do pracodawcy albo współfinansowane [10], a NIST przypisuje je pracownikowi. W dokumentach urzędu warto więc zdefiniować każdy użyty skrót, zamiast zakładać, że pracownik, wykonawca i audytor rozumieją go tak samo.

Tabela 2.1: Porównanie modeli własności z perspektywy urzędu

	Wyłącznie służbowe	COPE	BYOD i CYOD
Właściciel	urząd	urząd	pracownik
Zakres zarządzania	całe urządzenie	całe urządzenie, z zasadami użytku prywatnego	wyłącznie dane i aplikacje służbowe
Wymazanie	pełne	pełne, po uprzedzeniu o utracie danych prywatnych	tylko danych służbowych
Pochodzenie urządzenia	znane urzędowi	znane urzędowi	nieznane (BYOD) albo ograniczone do listy modeli (CYOD)
Główne ryzyko	koszt sprzętu i dwa telefony u pracownika	granica prywatności pracownika	brak kontroli nad stanem urządzenia
Podstawa w prawie pracy	narzędzie pracy pracodawcy	narzędzie pracy pracodawcy	przy pracy zdalnej innej niż okazjonalna art. 67^{24} § 2 KP; poza nią regulacja wewnętrzna



Rysunek 2.2: Modele własności urządzeń w dwóch wymiarach: kto jest właścicielem i jak szeroki jest dopuszczony użytek prywatny. Kolor pomarańczowy oznacza modele, w których urząd nie kontroluje pochodzenia urządzenia.

Tabela 2.1 i rysunek 2.2 nie wskazują modelu najlepszego. NIST zauważa, że przy BYOD i CYOD organizacja nie zna łańcucha dostaw urządzenia i nie wie, czy nie zostało ono zmodyfikowane, a przy modelu wyłącznie służbowym może dobrać sprzęt i przygotować jego konfigurację, zanim trafi do użytkownika (5.1.3.1 i 5.1.3.3) [2]. Dla stanowisk z dostępem do danych szczególnie chronionych, na przykład w ewidencji ludności, pomocy społecznej albo podatkach, argumenty te przemawiają za urządzeniem służbowym. Dla dostępu do poczty i kalendarza przez część pracowników model BYOD z zarządzaniem aplikacjami bywa wystarczający, o ile urząd zaakceptuje ryzyko opisane w analizie.

Rozdział 3

Podstawy prawne

Żaden przepis nie nakazuje jednostce samorządu terytorialnego zakupu systemu MDM. Przepisy nakładają obowiązki, których przedmiotem są informacje i systemy: zarządzanie ryzykiem, inwentaryzacja sprzętu, kontrola uprawnień, ochrona danych osobowych, rejestrowanie zdarzeń i obsługa incydentów. Urządzenie mobilne podlega tym obowiązkom tak samo jak stacja robocza w urzędzie. System MDM jest jednym ze środków technicznych, którymi urząd może je wykonać wobec urządzeń przenośnych. Ten rozdział opisuje wymagania.

Obowiązki wynikają z trzech reżimów, które działają równolegle i się nie wykluczają: ustawy o krajowym systemie cyberbezpieczeństwa, przepisów o informatyzacji podmiotów realizujących zadania publiczne wraz z Krajowymi Ramami Interoperacyjności oraz RODO. Czwarty obszar, prawo pracy, rozstrzyga, w jakim zakresie urząd może kontrolować urządzenie używane przez pracownika.

3.1 Ustawa o KSC po nowelizacji z 2026 r.

3.1.1 Nowelizacja i jej terminy

Ustawa z 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw została ogłoszona 2 marca 2026 r. i weszła w życie 3 kwietnia 2026 r. [11]. Wdraża do prawa polskiego dyrektywę NIS2 [12, 13] i w miejsce operatorów usług kluczowych wprowadza kategorie podmiotów kluczowych i podmiotów ważnych. Jednostki samorządu terytorialnego były objęte ustawą już w pierwotnym brzmieniu z 2018 r. jako podmioty publiczne (art. 4 pkt 7 w zw. z art. 21 i 22) [14]. Po nowelizacji dzielą się na podmioty kluczowe (załącznik nr 1) i podmioty ważne (załącznik nr 2). Zakres ich obowiązków jest różny.

Przepisy przejściowe rozkładają obowiązki w czasie (rysunek 3.1). Podmioty, które w dniu wejścia w życie nowelizacji spełniały przesłanki uznania za podmiot kluczowy albo ważny, realizują obowiązki z rozdziału 3 ustawy o krajowym systemie cyberbezpieczeństwa w terminie 12 miesięcy od tego dnia (art. 33 ust. 1 ustawy nowelizującej). Podmiot kluczowy przeprowadza pierwszy audyt w terminie 24 miesięcy (art. 33 ust. 2). Jednostka, która spełni przesłanki później, liczy te same terminy od dnia ich spełnienia (art. 16 ustawy o KSC). Dotyczy to na przykład urzędu gminy, który przekroczy próg zatrudnienia. Większość kar pieniężnych może zostać nałożona po raz pierwszy po upływie 2 lat od wejścia w życie nowelizacji. Chodzi o kary

z art. 73 ust. 1-4, art. 73a-73c i art. 76b (art. 35). Odroczenie nie obejmuje kary z art. 73 ust. 5 [11].

Wpis do wykazu podmiotów kluczowych i podmiotów ważnych przebiega dla samorządu inaczej niż dla przedsiębiorców. Podmioty publiczne, a więc jednostki samorządu z sektora "Podmioty publiczne" w załącznikach nr 1 i 2, minister właściwy do spraw informatyzacji wpisuje do wykazu z urzędu, na podstawie danych z rejestrów publicznych (art. 7a ust. 2 pkt 3 ustawy o KSC). Jednostka dostaje zawiadomienie o wpisie i wezwanie do uzupełnienia brakujących danych. Na uzupełnienie ma 6 miesięcy od doręczenia wezwania, pod rygorem kary pieniężnej. Dane uzupełnia wnioskiem o zmianę wpisu (art. 7b ust. 1, 2 i 4) [11]. Minister ogłosił okno wniosków od 7 maja do 3 października 2026 r. komunikatem z 8 kwietnia 2026 r., wydanym na podstawie art. 33 ust. 3 i art. 34 ust. 3 pkt 1 ustawy nowelizującej. Okno dotyczy podmiotów, które same składają wniosek o wpis, i wyłącza podmioty wpisane z urzędu. Korzystanie z systemu teleinformatycznego do zgłaszania incydentów podmioty rozpoczynają co do zasady w terminie od 12 czerwca 2026 r. do 3 kwietnia 2027 r. [15]

Rysunek 3.1: Terminy wynikające z nowelizacji ustawy o KSC i z utraty mocy rozporządzenia KRI. Daty liczone od 3 kwietnia 2026 r. na podstawie art. 33 i 35 ustawy nowelizującej; okno wniosków według komunikatu ministra.

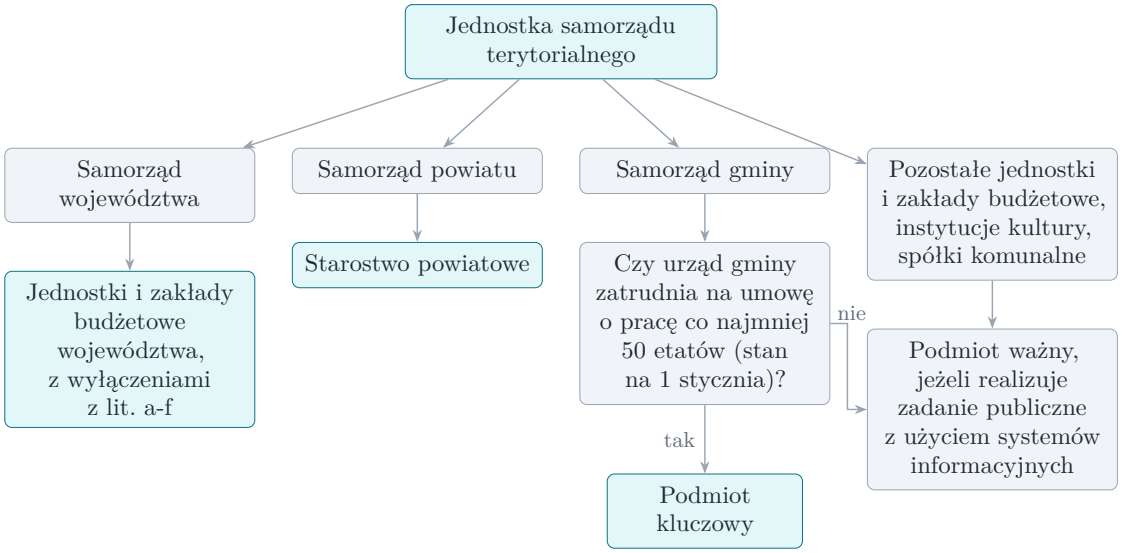
3.1.2 Podmioty kluczowe i ważne w samorządzie

Załącznik nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym nowelizacją wymienia w sektorze "Podmioty publiczne" trzy grupy jednostek samorządowych (rysunek 3.2) [11]:

- w samorządzie województwa: jednostki budżetowe i zakłady budżetowe, z wyłączeniem m.in. jednostek systemu oświaty, jednostek wspierania rodziny i pieczy zastępczej, części jednostek pomocy społecznej, wojewódzkich urzędów pracy i parków krajobrazowych (pkt 2 lit. a-f);
- w samorządzie powiatu: starostwo powiatowe (pkt 3);
- w samorządzie gminy: urząd gminy, jeżeli na dzień 1 stycznia danego roku zatrudnia na podstawie umowy o pracę co najmniej 50 osób w przeliczeniu na pełny wymiar czasu pracy (pkt 4).

Pozostałe samorządowe jednostki budżetowe i zakłady budżetowe, samorządowe instytucje kultury oraz spółki wykonujące zadania o charakterze użyteczności publicznej są podmiotami ważnymi, jeżeli realizują zadanie publiczne z wykorzystaniem systemów informacyjnych (art. 5 ust. 2 pkt 8 ustawy o KSC, załącznik nr 2, sektor "Podmioty publiczne") [11]. Dotyczy

to także urzędu gminy poniżej progu z pkt 4 oraz jednostek podległych, takich jak szkoły, ośrodki pomocy społecznej czy biblioteki. **Urząd gminy zatrudniający mniej niż 50 osób w przeliczeniu na etaty nie jest podmiotem kluczowym, ale jest podmiotem ważnym.** Podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w zakresie z załącznika nr 4 (art. 8 ust. 3), zgłasza incydenty poważne i uzupełnia dane w wykazie na wezwanie ministra, a obowiązki z KRI i RODO, opisane dalej, obowiązują go niezależnie od tego statusu.



Rysunek 3.2: Uproszczona ścieżka kwalifikacji jednostki samorządu według załączników nr 1 i 2. Schemat nie obejmuje przesłanek z innych sektorów, np. gospodarki komunalnej.

3.1.3 Wspólna obsługa i porozumienia

Nowelizacja dodaje w art. 16e ust. 5-9 możliwość zapewnienia wspólnej obsługi realizacji obowiązków z zakresu cyberbezpieczeństwa przez jednostkę samorządu oraz zawarcia przez jednostki samorządu porozumienia powierzającego te obowiązki jednej z nich [11]. Do wyznaczenia jednostki obsługującej stosuje się odpowiednio przepisy o wspólnej obsłudze z ustaw ustrojowych: art. 10a-10d ustawy o samorządzie gminnym, art. 6a-6d ustawy o samorządzie powiatowym i art. 8c-8f ustawy o samorządzie województwa. Podmioty obsługiwane współpracują z jednostką wyznaczoną, w szczególności przekazują jej informacje o incydentach (art. 16f).

Dla urządzeń mobilnych oznacza to, że jeden system MDM może obsługiwać urząd i jego jednostki organizacyjne albo kilka gmin, o ile podział odpowiedzialności wynika z aktu o wspólnej obsłudze lub z porozumienia. Rozdział 6 opisuje, co z tego wynika dla zamówienia.

3.1.4 Obowiązki kierownika jednostki

Nowelizacja przypisuje odpowiedzialność za cyberbezpieczeństwo kierownikowi podmiotu kluczowego lub ważnego. W urzędzie gminy jest nim wójt, burmistrz albo prezydent miasta, w starostwie starosta, w urzędzie marszałkowskim marszałek, a w jednostce podległej jej kierownik. Kierownik:

- ponosi odpowiedzialność za wykonywanie obowiązków także wtedy, gdy powierzył je innej osobie (art. 8c ust. 1 i 3);
- podejmuje decyzje dotyczące systemu zarządzania bezpieczeństwem informacji i planuje na nie środki finansowe (art. 8d pkt 1 i 2);
- raz w roku kalendarzowym przechodzi szkolenie (art. 8e ust. 1).

Osoba, która ma realizować zadania z art. 8 lub art. 11, przed ich rozpoczęciem przedstawia informację z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji (art. 8f ust. 1); urząd powinien ocenić, czy dotyczy to administratorów systemu MDM. Kierownikowi podmiotu publicznego grozi kara pieniężna do 100% otrzymywanego wynagrodzenia (art. 73a ust. 5) [11].

3.1.5 Wymogi dla podmiotu kluczowego

Podmiot kluczowy wdraża system zarządzania bezpieczeństwem informacji według art. 8 ust. 1 ustawy o KSC. Kilka jego elementów dotyczy urządzeń mobilnych bezpośrednio [11]:

- bezpieczeństwo łańcucha dostaw produktów ICT (pkt 2 lit. e);
- polityki stosowania kryptografii, w tym szyfrowania (lit. k);
- uwierzytelnianie wieloskładnikowe w stosownych przypadkach (lit. l);
- zarządzanie aktywami (lit. m) i polityki kontroli dostępu (lit. n);
- regularne aktualizacje oprogramowania zgodnie z zaleceniami producenta (pkt 5 lit. b).

3.1.6 Wymogi dla podmiotu ważnego będącego podmiotem publicznym

Załącznik nr 4 do ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym nowelizacją określa minimalny zakres systemu zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym, a więc dla samorządowych jednostek z załącznika nr 2 (art. 8 ust. 3) [11]. Część I pkt 2 wymaga kontrolowania podstawowych wersji używanych produktów ICT, a jeżeli to możliwe, korzystania z mechanizmów kontroli instalacji produktów ICT "na urządzeniach, w tym na urządzeniach mobilnych". Część pozostałych punktów pokrywa się z obowiązkami z KRI opisanymi niżej: inwentaryzacja produktów ICT (pkt 1), ochrona informacji przed kradzieżą i nieuprawnionym dostępem (pkt 3), minimalne uprawnienia i ich bezzwłoczne cofanie (pkt 4-7) oraz zasady bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość (pkt 8). Pkt 15 i 16 wymagają monitorowania cyklu życia produktów ICT i stosowania stabilnych wersji, co do których brak informacji o krytycznych podatnościach; na urządzeniach mobilnych realizuje to minimalna wersja systemu wymuszana przez MDM. Pozostałe punkty dotyczą m.in. poczty elektronicznej, kopii zapasowych i szkoleń.

Mechanizm kontroli instalacji na urządzeniach mobilnych to w praktyce funkcja systemu MDM albo MAM.

3.2 Krajowe Ramy Interoperacyjności

3.2.1 Obowiązki z § 19 i § 20

Rozporządzenie Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności [16] obowiązuje każdy podmiot realizujący zadania publiczne, niezależnie od statusu w ustawie o krajowym systemie cyberbezpieczeństwa. Zgodnie z § 19 ust. 1 podmiot taki opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji. Wymagania te uznaje się za spełnione, jeżeli system opracowano na podstawie normy PN-ISO/IEC 27001, a zabezpieczenia, zarządzanie ryzykiem i audyt oparto na normach z nią związanych (§ 19 ust. 3). Kilka obowiązków z § 19 ust. 2 dotyczy urządzeń mobilnych wprost albo przez konieczność:

- ustalenie zasad postępowania z informacjami, które minimalizują ryzyko kradzieży informacji i środków przetwarzania informacji, "w tym urządzeń mobilnych" (pkt 11);
- utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania, obejmującej ich rodzaj i konfigurację (pkt 2);
- okresowa analiza ryzyka utraty integralności, dostępności lub poufności informacji (pkt 3);
- bezzwłoczna zmiana uprawnień w przypadku zmiany zadań osób (pkt 5);
- ochrona informacji przed kradzieżą i nieuprawnionym dostępem, w tym przez środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych i aplikacji (pkt 7 lit. c);
- ustanowienie podstawowych zasad bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość (pkt 8);
- zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji w umowach serwisowych ze stronami trzecimi (pkt 10);
- dbałość o aktualizację oprogramowania, stosowanie mechanizmów kryptograficznych adekwatnie do zagrożeń i redukcja ryzyk wynikających z opublikowanych podatności (pkt 12 lit. a, d i f);
- bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji (pkt 13);
- okresowy audyt wewnętrzny bezpieczeństwa informacji, nie rzadziej niż raz na rok (pkt 14).

Paragraf 20 wymaga dokumentowania rozliczalności w dziennikach systemów, w tym dostępu do systemu z uprawnieniami administracyjnymi, do konfiguracji systemu i do danych chronionych prawnie, oraz przechowywania dzienników przez dwa lata, jeżeli przepisy odrębne nie stanowią inaczej (ust. 1, 2 i 4).

Wymóg z pkt 2 jest najbardziej konkretny. Inwentarz obejmujący konfigurację każdego telefonu i tabletu da się prowadzić ręcznie przy kilku urządzeniach, ale przy kilkudziesięciu zapis ręczny przestaje odpowiadać stanowi faktycznemu po pierwszej aktualizacji systemu operacyjnego. System MDM odczytuje wersję systemu, stan szyfrowania i zainstalowane aplikacje z samego urządzenia i robi to na bieżąco.

3.2.2 Zmiana podstawy prawnej KRI

Ustawa z 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw nie zawiera przepisu uchylającego rozporządzenie w sprawie KRI. Nadaje nowe brzmienie delegacji z art. 18 ustawy o informatyzacji (art. 1 pkt 19): Rada Ministrów ma określić w drodze rozporządzenia szczegółowe sposoby realizacji obowiązków z art. 13 ust. 1 pkt 1 i 2 oraz art. 14 ust. 1. Zmiana ta wchodzi w życie po upływie 18 miesięcy od dnia ogłoszenia ustawy (art. 17), a do tego czasu stosuje się przepisy wydane na podstawie dotychczasowego art. 18 (art. 15) [17]. Ustawa nie zachowuje rozporządzenia z 2024 r. w mocy po tej dacie, więc traci ono moc z wejściem w życie art. 1 pkt 19, a baza aktów prawnych Sejmu oznacza je jako akt uznany za uchylony z dniem 23 lutego 2027 r. [18]

Obowiązki opisane wyżej są więc właściwą podstawą planowania wdrożenia rozpoczynanego w 2026 r. Dokumentację na okres po lutym 2027 r. urząd powinien porównać z rozporządzeniem wydanym na podstawie nowego art. 18.

3.3 RODO

Służbowy telefon urzędnika przechowuje dane osobowe w poczcie, kontaktach, zdjęciach dokumentów i aplikacjach dziedzinowych. RODO nie wymienia urządzeń mobilnych, ale kilka jego przepisów przesądza o tym, jak urząd ma nimi zarządzać [19]:

- art. 5 ust. 1 lit. f wymaga przetwarzania danych w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed utratą;
- art. 24 ust. 1 zobowiązuje administratora do wdrożenia odpowiednich środków technicznych i organizacyjnych oraz do możliwości wykazania zgodności, co przy urządzeniach rozproszonych po terenie gminy w praktyce oznacza raport o ich stanie;
- art. 25 wymaga uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych, czyli przetwarzania wyłącznie danych niezbędnych do celu;
- art. 32 ust. 1 wymienia wprost szyfrowanie danych osobowych (lit. a), zdolność do zapewnienia poufności, integralności, dostępności i odporności systemów (lit. b) oraz regularne testowanie skuteczności środków (lit. d);
- art. 33 ust. 1 nakłada obowiązek zgłoszenia naruszenia organowi nadzorczemu bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po jego stwierdzeniu, chyba że naruszenie prawdopodobnie nie skutkuje ryzykiem dla praw lub wolności osób, a art. 34 obowiązek zawiadomienia osób, których dane dotyczą, gdy naruszenie może powodować wysokie ryzyko;

- art. 28 ust. 1 pozwala korzystać wyłącznie z podmiotów przetwarzających, które zapewniają wystarczające gwarancje; dostawca systemu MDM świadczonego jako usługa w chmurze jest takim podmiotem, bo przetwarza dane o urządzeniach i użytkownikach.

Utrata zaszyfrowanego telefonu, którego zawartość urząd może zdalnie wymazać, jest innym zdarzeniem niż utrata telefonu bez szyfrowania i bez możliwości zdalnego działania. Ocena, czy zdarzenie powoduje ryzyko naruszenia praw lub wolności osób fizycznych, należy do administratora w każdym przypadku osobno, ale od środków wdrożonych przed incydentem zależy, jakie fakty urząd będzie mógł w tej ocenie wykazać. Szyfrowanie ma tu skutek wprost przewidziany w RODO: jeżeli dane na utraconym urządzeniu były zaszyfrowane w sposób uniemożliwiający odczyt osobom nieuprawnionym, zawiadomienie osób, których dane dotyczą, nie jest wymagane (art. 34 ust. 3 lit. a). Ocena ryzyka i ewentualne zgłoszenie do organu nadzorczego pozostają.

3.3.1 Ocena skutków dla ochrony danych

Art. 35 ust. 1 RODO wymaga oceny skutków dla ochrony danych, gdy przetwarzanie, w szczególności z użyciem nowych technologii, może powodować wysokie ryzyko. Prezes UODO ogłosił na podstawie art. 35 ust. 4 wykaz rodzajów operacji wymagających takiej oceny. Pozycja 12 wykazu dotyczy przetwarzania danych lokalizacyjnych. Jako przykłady podaje przetwarzanie danych w kontekście pracy w domu i pracy zdalnej oraz przetwarzanie danych lokalizacyjnych pracowników. Pozycja 3 wymienia jako przykład zakłady pracy prowadzące monitoring systemów informatycznych, poczty elektronicznej i używanego oprogramowania. Co do zasady ocena jest wymagana, gdy przetwarzanie spełnia co najmniej dwa kryteria z wykazu [20]. System MDM z włączoną lokalizacją urządzeń albo obejmujący urządzenia prywatne należy więc przed uruchomieniem przeanalizować pod kątem obowiązku oceny skutków. Wyłączenie funkcji lokalizacji w stałej pracy systemu, z możliwością jej użycia tylko po zgłoszeniu utraty urządzenia, ogranicza zakres tej oceny.

3.4 Mapa wymogów na funkcje systemu

Tabela 3.1 zestawia wymogi z podrozdziałów 3.1-3.3 z funkcjami, którymi system MDM może je wykonywać. Kolumna środkowa nie jest katalogiem obowiązków: przepis wymaga skutku, a funkcja jest jednym ze sposobów jego osiągnięcia.

3.5 Prawo pracy

System MDM daje administratorowi wgląd w urządzenie, z którego korzysta pracownik. Kodeks pracy wyznacza granice tego wglądu w dwóch miejscach [21].

Pierwsze to przepisy o monitoringu. Art. 22^3 § 1 pozwala pracodawcy wprowadzić kontrolę służbowej poczty elektronicznej, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych narzędzi pracy, a § 2 zastrzega, że kontrola nie może naruszać tajemnicy korespondencji ani innych dóbr osobistych pracownika. Zgodnie z § 4 przepisy te stosuje się odpowiednio do innych form monitoringu, jeśli ich zastosowanie jest konieczne do realizacji tych samych celów.

Tabela 3.1: Wymogi prawne i odpowiadające im funkcje systemu MDM

Wymóg	Funkcja systemu MDM	Podstawa
Aktualny inwentarz sprzętu z konfiguracją	automatyczny odczyt modelu, wersji systemu, stanu szyfrowania, aplikacji; eksport inwentarza	KRI § 19 ust. 2 pkt 2
Zasady bezpiecznej pracy mobilnej	profile konfiguracji: blokada ekranu, szyfrowanie, ograniczenia, sieć VPN	KRI § 19 ust. 2 pkt 8
Zmiana uprawnień przy zmianie zadań	przypisanie urządzenia do użytkownika i grupy; odebranie dostępu przy odejściu	KRI § 19 ust. 2 pkt 5
Szyfrowanie danych	wymuszenie i raport szyfrowania pamięci	RODO art. 32 ust. 1 lit. a; KRI § 19 ust. 2 pkt 12 lit. d
Wykazanie zgodności	raporty zgodności z polityką, historia zmian	RODO art. 24 ust. 1
Ochrona przed utratą danych i urządzenia	zdalne zablokowanie i wymazanie; oddzielenie danych służbowych	RODO art. 5 ust. 1 lit. f; KRI § 19 ust. 2 pkt 11
Rozliczalność działań administratorów	dziennik działań w konsoli, eksport do systemu zbierania logów	KRI § 20 ust. 1 i 2
Zgłaszanie incydentów	alerty o niezgodności, urządzeniu utraconym lub zmodyfikowanym	KRI § 19 ust. 2 pkt 13; RODO art. 33; KSC art. 11 ust. 1 pkt 4-4c (kluczowy); pkt 4a w zw. z art. 12c (ważny)
Aktualizacje i podatności	wymuszenie aktualizacji, blokada wersji bez wsparcia	KRI § 19 ust. 2 pkt 12 lit. a i f; KSC art. 8 ust. 1 pkt 5 lit. b (kluczowy); zał. 4 cz. I pkt 15-16 (ważny)
Kontrola instalacji produktów ICT na urządzeniach mobilnych	lista aplikacji dozwolonych, blokada instalacji spoza katalogu	KSC zał. 4 cz. I pkt 2 (ważny)

Cele, zakres i sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy, a w obwieszczeniu tylko wtedy, gdy pracodawca nie jest objęty układem ani obowiązany do ustalenia regulaminu. Pracowników informuje się nie później niż 2 tygodnie przed uruchomieniem monitoringu, a nowych pracowników na piśmie przed dopuszczeniem do pracy (art. 22^2 § 6-8, stosowane na podstawie art. 22^3 § 3). Pracodawca zatrudniający co najmniej 50 pracowników wprowadza regulamin pracy (art. 104 § 1^1), ustalany w uzgodnieniu z zakładową organizacją związkową (art. 104^2 § 1).

Nie każda funkcja systemu MDM jest monitoringiem pracownika. Sprawdzenie, czy urządzenie ma włączone szyfrowanie i aktualny system, dotyczy urządzenia, a nie osoby. Odczyt lokalizacji, listy aplikacji prywatnych albo historii przeglądania może już być inną formą monitoringu w rozumieniu art. 22^3 § 4. Regulamin powinien wymieniać funkcje, z których urząd korzysta, i te, które są wyłączone.

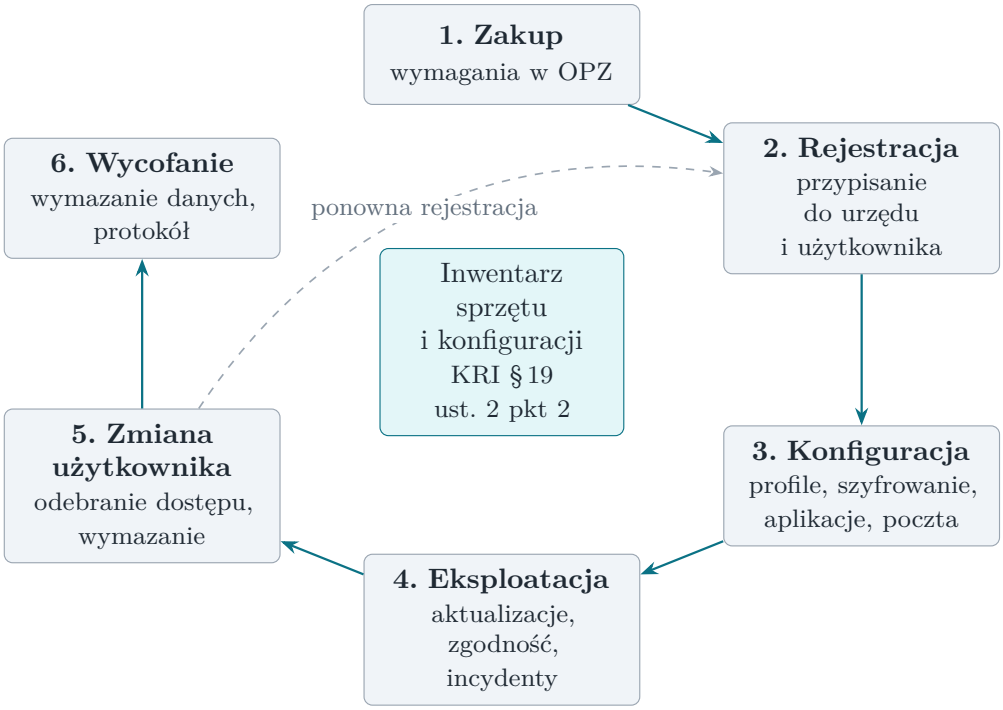
Drugie miejsce to przepisy o pracy zdalnej. Porozumienie albo regulamin pracy zdalnej określa m.in. zasady kontroli przestrzegania wymogów bezpieczeństwa i ochrony informacji oraz zasady instalacji, inwentaryzacji, konserwacji i aktualizacji oprogramowania powierzonych pracownikowi narzędzi pracy (art. 67^{20} § 6 pkt 7 i 8). Pracodawca określa procedury ochrony danych osobowych i w miarę potrzeby przeprowadza szkolenie (art. 67^{26} § 1). Strony mogą ustalić, że pracownik wykonuje pracę zdalną na własnych narzędziach, a wtedy przysługuje mu ekwiwalent pieniężny albo ryczałt (art. 67^{24} § 2-4). Kontrola w miejscu wykonywania pracy zdalnej nie może naruszać prywatności pracownika i innych osób (art. 67^{28} § 1 i 2). Przy okazjonalnej pracy zdalnej, wykonywanej na wniosek pracownika do 24 dni w roku, przepisów art. 67^{19}-67^{24} się nie stosuje, a kontrolę przestrzegania wymogów bezpieczeństwa i ochrony informacji prowadzi się na zasadach ustalonych z pracownikiem (art. 67^{33} § 2 i 3).

Przepisy o pracy zdalnej są jedyną regulacją w prawie pracy, która wprost przewiduje używanie prywatnego sprzętu pracownika. Model BYOD poza pracą zdalną wymaga więc szczególnie starannego uregulowania w wewnętrznych aktach urzędu, co opisuje rozdział 5.

Rozdział 4

Cykl życia urządzenia

Urządzenie mobilne przechodzi w urzędzie przez sześć etapów, od zakupu do wycofania (rysunek 4.1). Obowiązek prowadzenia aktualnego inwentarza sprzętu wraz z konfiguracją (KRI § 19 ust. 2 pkt 2) obejmuje każdy z tych etapów [16]. Publikacja NIST SP 800-124 Rev. 2 opisuje ten sam cykl od strony organizacji: od rozpoznania potrzeb i inwentaryzacji istniejących urządzeń (5.1), przez ocenę ryzyka (5.2), wdrożenie (5.3) i eksploatację (5.4), po wycofanie lub ponowne użycie urządzenia (5.5) [2].



Rysunek 4.1: Cykl życia urządzenia mobilnego w urzędzie. Linia przerywana oznacza powrót urządzenia do rejestracji po wymazaniu przy zmianie użytkownika; każdy etap zmienia zapis w inwentarzu.

4.1 Rozpoznanie stanu wyjściowego

Wdrożenie zaczyna się od ustalenia, jakie urządzenia już mają dostęp do danych urzędu. NIST zaleca połączenie dwóch źródeł: zapytania pracowników o urządzenia, których używają, i przeglądu urządzeń widocznych w sieci organizacji (5.1.2) [2]. W urzędzie trzecim źródłem są logi serwera poczty, które pokazują urządzenia synchronizujące skrzynki służbowe. Taki przegląd może ujawnić telefony prywatne, na których pracownicy sami skonfigurowali pocztę służbową, oraz urządzenia byłych pracowników, które wciąż mają aktywne połączenie.

4.2 Zakup

Wymagania bezpieczeństwa wobec urządzenia są najtańsze do spełnienia przed zakupem. Opis przedmiotu zamówienia na telefony i tablety powinien obejmować co najmniej: zgodność z programem rejestracji urządzeń dla organizacji oferowanym przez twórcę systemu operacyjnego, szyfrowanie pamięci, deklarowany przez producenta okres dostarczania aktualizacji bezpieczeństwa oraz możliwość zarejestrowania urządzenia w systemie MDM używanym przez urząd. Dla smartfonów i tabletów wprowadzanych do obrotu od 20 czerwca 2025 r. część tych cech wynika z prawa Unii. Rozporządzenie Komisji (UE) 2023/1670 wymaga domyślnego szyfrowania danych użytkownika (podrozdział 4.7) i określa zasady udostępniania aktualizacji systemu operacyjnego. Przez co najmniej 5 lat od zakończenia wprowadzania modelu do obrotu producent, który zapewnia aktualizacje zabezpieczeń, aktualizacje korygujące lub aktualizacje funkcji, udostępnia je bezpłatnie wszystkim egzemplarzom tego modelu. Aktualizacje zabezpieczeń i korygujące muszą trafić do użytkownika najpóźniej 4 miesiące po publicznym udostępnieniu kodu źródłowego aktualizacji systemu bazowego. Jeżeli kodu nie udostępniono, termin biegnie od wydania tej aktualizacji przez dostawcę systemu operacyjnego albo na innym produkcie tej samej marki (załącznik II część B sekcja 1.2 pkt 6 lit. a i c, część D sekcja 1.2 pkt 5 lit. a i c) [22]. Obowiązek dotyczy aktualizacji, które producent zapewnia, dlatego deklarowany okres ich wydawania dla oferowanego modelu nadal warto ująć w opisie przedmiotu zamówienia. Urząd sprawdza też, czy typ urządzenia nie jest objęty decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka (rozdział 6). NIST zaleca uwzględnienie przy wyborze urządzeń ich łańcucha dostaw i cech bezpieczeństwa (4.3.4, 5.1.4) [2]. Zasady opisu przedmiotu zamówienia bez wskazywania znaków towarowych omawia rozdział 6.

4.3 Rejestracja

Rejestracja przypisuje urządzenie do urzędu w systemie MDM i do konkretnego użytkownika. Twórcy głównych systemów operacyjnych oferują organizacjom programy rejestracji automatycznej: urządzenie kupione przez organizację trafia na jej konto, a po pierwszym uruchomieniu łączy się z systemem MDM bez udziału użytkownika. Przy odpowiedniej konfiguracji taka rejestracja ma dwie przewagi nad ręczną: użytkownik nie może jej pominąć ani cofnąć, a po przywróceniu ustawień fabrycznych urządzenie ponownie łączy się z systemem urzędu, co obniża wartość skradzionego telefonu. Warunki programów i dostępne ustawienia różnią się między platformami, więc wymagania wobec rejestracji trzeba sprawdzić dla każdej platformy używanej w urzędzie.

Rejestracja urządzenia prywatnego przebiega inaczej: to pracownik instaluje aplikację albo profil i to on może zakończyć zarządzanie. Przy modelu BYOD warunkiem dostępu do danych służbowych jest więc zwykle aktywne zarządzanie aplikacjami. Samo urządzenie pozostaje pod kontrolą pracownika.

4.4 Konfiguracja

Konfiguracja przenosi politykę urzędu na ustawienia urządzenia. NIST wymienia jako typowe ustawienia wymuszane przez EMM m.in.: zarządzanie interfejsami bezprzewodowymi, ograniczenie dostępu do aparatu i pamięci wymiennej, wykrywanie zmian w zatwierdzonej konfiguracji bazowej, blokowanie dostępu urządzeniom z nieaktualnym systemem albo ze zdjętymi zabezpieczeniami producenta, wymóg hasła i automatycznej blokady ekranu, szyfrowanie komunikacji i danych przechowywanych oraz zdalne wymazanie (4.2.1.1-4.2.1.3) [2]. Przed wydaniem urządzeń użytkownikom konfigurację sprawdza się w pilotażu opisanym w rozdziale 7.

Tabela 4.1 pokazuje, jak takie ustawienia zapisać w polityce, żeby każde miało wskazaną podstawę.

Tabela 4.1: Przykładowa polityka dla urządzeń wyłącznie służbowych. Ustawienia wynikające wyłącznie z decyzji urzędu są tak oznaczone, co ułatwia ich przegląd podczas audytu. Wartości są przykładowe.

Ustawienie	Wartość	Podstawa
Blokada ekranu	kod PIN co najmniej 6 cyfr, blokada po 2 minutach	RODO art. 32
Szyfrowanie pamięci	wymagane	RODO art. 32 ust. 1 lit. a
Minimalna wersja systemu	wspierana przez producenta	KRI § 19 ust. 2 pkt 12 lit. a
Źródła aplikacji	wyłącznie katalog zatwierdzony przez urząd	decyzja urzędu; dla podmiotu ważnego KSC zał. 4 cz. I pkt 2
Kopia danych w prywatnej chmurze	zablokowana	decyzja urzędu
Utrata urządzenia	zdalne zablokowanie i wymazanie	KRI § 19 ust. 2 pkt 7 i 11
Brak kontaktu z serwerem	alert po 14 dniach	decyzja urzędu

4.5 Eksploatacja

Na etapie eksploatacji system MDM pracuje w tle, a praca administratora polega na reagowaniu na odchylenia: urządzenie z wyłączonym szyfrowaniem, zaległa aktualizacja, urządzenie, które od dwóch tygodni nie łączyło się z serwerem. NIST zaleca szybkie wdrażanie aktualizacji oprogramowania (4.3.6), okresowe audyty obejmujące infrastrukturę mobilną i system zarządzania (5.4.1) oraz przyjęcie polityk bezpieczeństwa i prywatności dotyczących korzystania z urządzeń (5.4.2) [2]. KRI wymaga audytu wewnętrznego bezpieczeństwa informacji nie rzadziej niż raz na rok (§ 19 ust. 2 pkt 14) [16].

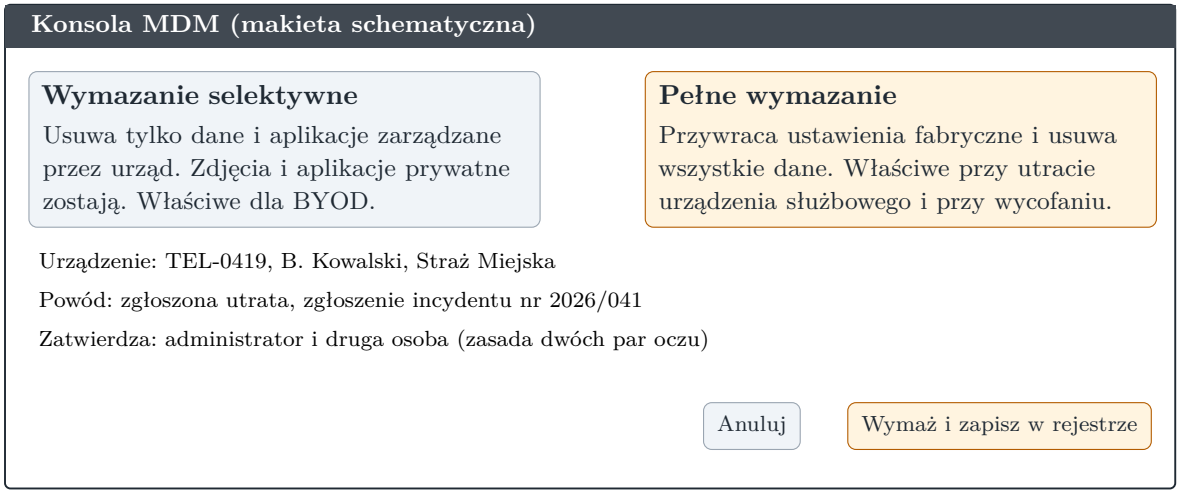
Tabela 4.2 pokazuje fragment inwentarza w układzie, który odpowiada zakresowi inwentaryzacji z KRI: rodzaj sprzętu i jego konfiguracja.

Tabela 4.2: Przykładowy inwentarz urządzeń mobilnych (dane fikcyjne). Urządzenie w magazynie pozostaje w inwentarzu, bo nadal jest mieniem urzędu.

Urządzenie	Użytkownik	Komórka	System	Szyfrowanie	Zgodność
TEL-0412	A. Nowak	Wydział Podatków	aktualny	włączone	zgodne
TEL-0419	B. Kowalski	Straż Miejska	aktualny	włączone	zgodne
TAB-0107	C. Wiśniewska	Wydział Geodezji	nieaktualny	włączone	niezgodne
TEL-0433	D. Wójcik	Sekretariat	aktualny	wyłączone	niezgodne
TAB-0111	kiosk, hol	Biuro Obsługi	aktualny	włączone	zgodne
TEL-0440	nieprzypisane	magazyn IT	nie dotyczy	nie dotyczy	w magazynie

4.6 Zmiana użytkownika

Zmiana stanowiska albo odejście pracownika wymaga bezzwłocznej zmiany uprawnień (KRI § 19 ust. 2 pkt 5) [16]. Dla urządzenia oznacza to trzy kroki: odebranie dostępu do zasobów urzędu na koncie użytkownika, wymazanie urządzenia (rysunek 4.2) i ponowną rejestrację dla nowego użytkownika. Odebranie dostępu na koncie idzie pierwsze, bo wymazanie jednego urządzenia nie kończy sesji tej samej osoby na innych urządzeniach. NIST zaleca wymazanie urządzenia przed wydaniem go innemu użytkownikowi (4.2.1.3) [2].



Rysunek 4.2: Makieta schematyczna decyzji o wymazaniu. Rozróżnienie wymazania selektywnego i pełnego odpowiada podziałowi na urządzenia prywatne i służbowe; zatwierdzenie przez drugą osobę ogranicza skutki przejęcia konta administratora.

4.7 Wycofanie

Wycofanie urządzenia z użytku to etap, na którym dane mogą opuścić urząd niezauważone. NIST wyjaśnia, że techniki stosowane do nośników magnetycznych są nieskuteczne wobec pamięci półprzewodnikowej urządzeń mobilnych, a bezpieczne usunięcie danych polega na

przywróceniu ustawień fabrycznych, które niszczy klucz szyfrowania pamięci (wymazanie kryptograficzne). Warunkiem jest włączenie szyfrowania całego urządzenia przed jego wydaniem. Smartfony i tablety wprowadzane do obrotu od 20 czerwca 2025 r. szyfrują dane użytkownika w pamięci wewnętrznej domyślnie, losowym kluczem. Mają też funkcję przywracania ustawień fabrycznych, która domyślnie usuwa w sposób bezpieczny klucz szyfrowania i generuje nowy (rozporządzenie 2023/1670, załącznik II część B i D sekcja 1.1 pkt 6 lit. a i b) [22]. Przywrócenie ustawień fabrycznych nie usuwa danych z karty SIM ani z karty pamięci, które należy wyjąć i zniszczyć, a urząd powinien sprawdzić, czy klucz szyfrowania nie jest przechowywany w kopii poza urządzeniem (5.5) [2].

Z wycofania sporządza się protokół: identyfikator urządzenia z inwentarza, data i sposób usunięcia danych, postępowanie z kartami SIM i pamięci, osoba wykonująca i osoba zatwierdzająca. Wzór listy kontrolnej zawiera załącznik A.

Rozdział 5

Polityka urządzeń mobilnych

System MDM wykonuje zasady, których sam nie ustala. KRI wymaga ustanowienia podstawowych zasad bezpiecznej pracy przy przetwarzaniu mobilnym (§ 19 ust. 2 pkt 8) [16], a przepisy prawa pracy wymagają, by zakres kontroli nad urządzeniem był pracownikom znany przed jej rozpoczęciem [21]. Zasady bezpiecznej pracy mobilnej mogą wejść do dokumentacji systemu zarządzania bezpieczeństwem informacji wydanej zarządzeniem kierownika jednostki. Cele, zakres i sposób monitoringu muszą jednak trafić do regulaminu pracy, ustalanego w uzgodnieniu z zakładową organizacją związkową (art. 104^2 § 1 KP), albo do układu zbiorowego pracy; obwieszczenie wchodzi w grę tylko u pracodawcy, który nie ma obowiązku ustalenia regulaminu. Przy pracy zdalnej właściwe jest porozumienie albo regulamin pracy zdalnej (art. 67^{20} KP). Polityka urządzeń mobilnych odsyła do tych aktów, ale ich nie zastępuje. Wzór struktury polityki zawiera załącznik B.

5.1 Klasyfikacja informacji

Zasady dla urządzeń zależą od tego, jakie informacje mają być na nich dostępne. Urząd, który nie sklasyfikował informacji, nie odpowie na podstawowe pytanie polityki: czy dany rodzaj danych może trafić na telefon, a jeżeli tak, to na jaki. W praktyce wystarczają trzy grupy:

- informacje publiczne i wewnętrzne o niskiej wrażliwości, na przykład kalendarz spotkań czy komunikaty organizacyjne;
- dane osobowe i informacje chronione na podstawie przepisów szczególnych, na przykład w sprawach podatkowych, pomocy społecznej czy ewidencji ludności;
- informacje, dla których urząd wyklucza przetwarzanie na urządzeniach mobilnych.

Polityka przypisuje każdej grupie dopuszczalne modele urządzeń z rozdziału 2.

5.2 Zakres zarządzania i prywatność

Polityka powinna wymieniać funkcje systemu MDM, z których urząd korzysta, oraz te, które są wyłączone. Podrozdział 3.5 wyjaśnia, dlaczego odczyt lokalizacji czy listy aplikacji prywatnych może być inną formą monitoringu w rozumieniu Kodeksu pracy. Tabela 5.1 pokazuje przykładowy podział.

Tabela 5.1: Przykładowy zakres zarządzania w polityce urzędu

Funkcja	Urządzenie służbowe	Urządzenie prywatne
Odczyt modelu, wersji systemu, stanu szyfrowania	tak	tak, w zakresie warunków dostępu
Wymuszenie blokady ekranu i szyfrowania	tak	tak, jako warunek dostępu
Instalacja i usunięcie aplikacji służbowych	tak	tak
Lista aplikacji prywatnych	po analizie, gdy użytek prywatny jest dopuszczony	nie
Lokalizacja urządzenia	tylko po zgłoszeniu utraty	nie
Pełne wymazanie	tak	nie
Wymazanie danych służbowych	tak	tak
Dostęp do treści prywatnych (zdjęcia, wiadomości)	nie	nie

Tabela nie jest rozstrzygnięciem prawnym. Pokazuje zasadę, według której każdy urząd powinien sporządzić własną: funkcja dotyczy albo urządzenia, albo osoby, a funkcje dotyczące osoby wymagają podstawy, celu i uprzedzenia pracownika. Przy funkcji lokalizacji trzeba też rozważyć obowiązek oceny skutków dla ochrony danych, opisany w podrozdziale 3.3.

5.3 Urządzenia prywatne

Jeżeli urząd dopuszcza korzystanie z urządzeń prywatnych, polityka powinna rozstrzygać co najmniej:

- jakie dane służbowe i jakie aplikacje są dostępne na urządzeniu prywatnym, a jakie wyłącznie na służbowym;
- jakie minimalne warunki musi spełniać urządzenie: wspierana wersja systemu, blokada ekranu, szyfrowanie, brak zdjętych zabezpieczeń producenta;
- że urząd zarządza wyłącznie danymi i aplikacjami służbowymi i może usunąć tylko je;
- co pracownik robi w razie utraty urządzenia, zmiany telefonu i zakończenia zatrudnienia;
- wysokość i zasady ekwiwalentu pieniężnego, który przysługuje pracownikowi używającemu własnego sprzętu przy pracy zdalnej, albo ryczałtu, który może go zastąpić (art. 67^{24} § 3 i 4 KP); przy okazjonalnej pracy zdalnej te przepisy nie mają zastosowania (art. 67^{33} § 2).

Pisemne potwierdzenie przystąpienia do programu urządzeń prywatnych i zapoznania się z zakresem zarządzania dokumentuje, że pracownik zna warunki. Nie jest natomiast podstawą przetwarzania danych w rozumieniu RODO: motyw 43 RODO wskazuje, że zgoda nie powinna stanowić ważnej podstawy prawnej, gdy między osobą a administratorem występuje wyraźny brak równowagi, w szczególności gdy administrator jest organem publicznym [19]. Podstawą przetwarzania danych w systemie MDM jest co do zasady wypełnienie obowiązku prawnego (art. 6 ust. 1 lit. c RODO) wynikającego z KRI i ustawy o KSC, a w zakresie monitoringu przepisy art. 22^3 KP. Prawnie uzasadniony interes (art. 6 ust. 1 lit. f) nie jest dostępny organowi publicznemu w ramach realizacji jego zadań (art. 6 ust. 1 akapit drugi RODO).

Podstawę w konkretnym urzędzie ustala administrator, z udziałem inspektora ochrony danych, który doradza i monitoruje przestrzeganie przepisów (art. 39 ust. 1 lit. a i b RODO).

Przetwarzanie danych w systemie MDM administrator wpisuje do rejestru czynności przetwarzania (art. 30 ust. 1 RODO). Zwolnienie podmiotów zatrudniających mniej niż 250 osób nie obejmuje przetwarzania, które nie ma charakteru sporadycznego, a system MDM przetwarza dane stale (art. 30 ust. 5). Pracownikom administrator przekazuje przy pozyskiwaniu danych informacje z art. 13 ust. 1 RODO, w tym o celach i podstawie prawnej przetwarzania [19].

5.4 Szkolenie użytkowników

KRI wymaga szkolenia osób zaangażowanych w przetwarzanie informacji (§ 19 ust. 2 pkt 6) [16], a NIST wymienia edukację użytkowników jako jeden ze środków ograniczających zagrożenia mobilne (4.3.10) [2]. Szkolenie dla użytkowników urządzeń mobilnych powinno obejmować trzy tematy praktyczne: rozpoznawanie wiadomości wyłudzających dane logowania, w tym przez SMS; postępowanie po utracie urządzenia, z numerem telefonu i adresem zgłoszenia; oraz to, czego urząd na urządzeniu nie widzi i nie robi.

Rozdział 6

Zakup systemu

6.1 Tryb zamówienia

Ustawę Prawo zamówień publicznych stosuje się do zamówień klasycznych o wartości równej lub przekraczającej 170 000 zł udzielanych przez zamawiających publicznych (art. 2 ust. 1 pkt 1 Pzp w brzmieniu obowiązującym od 1 stycznia 2026 r.) [23]. W latach 2026-2027 próg unijny dla dostaw i usług udzielanych przez zamawiających innych niż administracja rządowa centralna wynosi 216 000 euro, czyli 930 960 zł według kursu określonego w obwieszczeniu Prezesa Urzędu Zamówień Publicznych [24].

Wartość zamówienia na system MDM obejmuje licencje albo subskrypcję na cały okres umowy, usługi wdrożeniowe, szkolenia i wsparcie. Przy subskrypcji wieloletniej łączna wartość jest wielokrotnością ceny rocznej. To może zmienić tryb. Zamawiający nie może zaniżać wartości zamówienia w celu uniknięcia stosowania przepisów ustawy (art. 29 ust. 1 Pzp). Nie może też dzielić zamówienia na odrębne zamówienia, jeżeli prowadzi to do niestosowania przepisów ustawy, chyba że jest to uzasadnione obiektywnymi przyczynami (art. 29 ust. 2) [23].

6.2 Opis przedmiotu zamówienia

Przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję. Zakaz dotyczy w szczególności wskazania znaków towarowych, patentów lub pochodzenia, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów (art. 99 ust. 4 Pzp). Wskazanie znaku towarowego jest dopuszczalne, gdy zamawiający nie może opisać przedmiotu w wystarczająco precyzyjny i zrozumiały sposób. Wskazaniu towarzyszą wtedy wyrazy "lub równoważny" (art. 99 ust. 5), a zamawiający podaje w opisie kryteria oceny równoważności (art. 99 ust. 6). Zamówienia przeznaczone do użytku osób fizycznych, w tym pracowników zamawiającego, opisuje się z uwzględnieniem wymagań w zakresie dostępności dla osób niepełnosprawnych oraz projektowania z przeznaczeniem dla wszystkich użytkowników. Wyjątkiem jest sytuacja, w której nie jest to uzasadnione charakterem przedmiotu zamówienia (art. 100 ust. 1) [23]. Dotyczy to konsoli administratora i aplikacji instalowanych na urządzeniach pracowników.

System MDM daje się opisać funkcjonalnie: urząd określa, co system ma robić, i nie wskazuje nazwy produktu. Pzp przewiduje ten sposób wprost jako określenie wymagań

dotyczących wydajności lub funkcjonalności, pod warunkiem że parametry są dostatecznie precyzyjne (art. 101 ust. 1 pkt 1) [23]. Opis można zbudować z trzech warstw:

1. wymagania wynikające z prawa, przełożone na funkcje z tabeli 3.1: inwentarz z konfiguracją, wymuszanie szyfrowania, zdalne wymazanie, rejestr działań administratorów;
2. wymagania wynikające z przyjętego modelu własności: pełne zarządzanie urządzeniem służbowym, zarządzanie tylko danymi służbowymi na urządzeniu prywatnym;
3. wymagania środowiskowe: obsługiwane platformy i minimalne wersje systemów, integracja z katalogiem tożsamości i z systemem zbierania logów używanym przez urząd, liczba urządzeń z zapasem.

Załącznik C zawiera listę kryteriów, z której można ułożyć opis przedmiotu zamówienia. Lista nie odwołuje się do żadnego produktu i wymaga dostosowania do urzędu.

6.3 Dostawcy wysokiego ryzyka

Nowelizacja KSC wprowadziła postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Prowadzi je minister właściwy do spraw informatyzacji wobec dostawców, z których korzystają m.in. podmioty kluczowe i ważne (art. 67b ust. 1 pkt 1 ustawy o KSC). Po wydaniu decyzji te podmioty nie wprowadzają do użytkowania objętych nią typów produktów ICT, usług i procesów. Już używane wycofują najpóźniej w ciągu 7 lat od ogłoszenia decyzji w Monitorze Polskim (art. 67c ust. 1). Podmioty stosujące Pzp nie mogą ich nabywać (art. 67c ust. 4) [11]. Zamawiający odrzuca ofertę obejmującą produkt ICT, którego typ określono w takiej decyzji, albo usługę lub proces ICT w niej określone (art. 226 ust. 1 pkt 19 Pzp). Odrzuca też ofertę obejmującą produkt, usługę albo proces ICT wskazane w rekomendacji z art. 33 ust. 4 ustawy o KSC (art. 226 ust. 1 pkt 17 Pzp) [23]. Przed ogłoszeniem postępowania na system MDM albo na urządzenia mobilne urząd sprawdza więc aktualne decyzje i rekomendacje.

6.4 Dane, umowa i wyjście z umowy

System MDM przetwarza dane osobowe pracowników: imię i nazwisko, konto, identyfikatory urządzenia, a przy włączonych funkcjach także lokalizację. Jeżeli system działa jako usługa w infrastrukturze wykonawcy, wykonawca jest podmiotem przetwarzającym. Urząd może korzystać wyłącznie z podmiotów zapewniających wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 28 ust. 1 RODO) [19]. Projekt umowy powierzenia przetwarzania, o treści wymaganej przez art. 28 ust. 3 RODO, powinien być częścią dokumentacji zamówienia. Wykonawca zna wtedy jej warunki przed złożeniem oferty.

KRI wymaga zawierania w umowach serwisowych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji (§ 19 ust. 2 pkt 10) [16]. W umowie na system MDM szczególnego znaczenia nabierają postanowienia o:

- miejscu przetwarzania danych i ewentualnym przekazaniu ich poza Europejski Obszar Gospodarczy;

- dostępie urzędu do rejestru działań administratorów, także działań personelu wykonawcy;
- eksporcie inwentarza i konfiguracji w formacie umożliwiającym przeniesienie do innego systemu przy zakończeniu umowy;
- obowiązku wykonawcy informowania o incydentach dotyczących systemu w czasie, który pozwoli urzędowi dotrzymać terminów z ustawy o KSC (24 godziny na wczesne ostrzeżenie w podmiocie kluczowym, 72 godziny na zgłoszenie incydentu poważnego, art. 11 ust. 1 pkt 4 i 4a) i ocenić naruszenie ochrony danych (art. 33 RODO); jako podmiot przetwarzający wykonawca zgłasza naruszenie administratorowi bez zbędnej zwłoki (art. 33 ust. 2 RODO);
- własności kont urzędu w programach rejestracji urządzeń twórców systemów operacyjnych, które powinny należeć do urzędu, a nie do wykonawcy.

Ostatni punkt wynika z konstrukcji opisanej w rozdziale 2: konto w programie rejestracji decyduje, z którym systemem MDM połączy się nowe urządzenie. Jeżeli należy do wykonawcy, zmiana wykonawcy wymaga jego współpracy.

6.5 Wspólny zakup i wspólna obsługa

Art. 16e ust. 5-9 ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym nowelizacją z 2026 r. pozwala jednostkom samorządu zapewnić wspólną obsługę obowiązków z zakresu cyberbezpieczeństwa albo powierzyć ich realizację jednej jednostce na podstawie porozumienia [11]. Wspólny system MDM dla gminy i jej jednostek organizacyjnych albo dla kilku gmin musi pozwalać rozdzielić urządzenia i uprawnienia administratorów według jednostek, co warto ująć w opisie przedmiotu zamówienia. Wymaga to spójności trzech dokumentów: porozumienia albo aktu o wspólnej obsłudze, umowy z wykonawcą i ustaleń o danych osobowych między jednostkami. Rolę każdej jednostki wobec danych osobowych, powierzenie (art. 28 RODO) albo współadministrowanie (art. 26 RODO), ustala porozumienie.

6.6 Finansowanie

Program grantowy "Cyberbezpieczny Samorząd", prowadzony przez Centrum Projektów Polska Cyfrowa, jest w fazie realizacji i rozliczenia: komunikat z 16 czerwca 2026 r. dopuszcza przedłużenie realizacji grantu do 30 września 2026 r. aneksem do umowy [25].

Kolejnym źródłem jest nabór na Lokalne Centra Cyberbezpieczeństwa, ogłoszony przez Centrum Projektów Polska Cyfrowa w ramach działania 4.1 programu Fundusze Europejskie na Rozwój Cyfrowy. O dotację mogą ubiegać się gminy, powiaty i województwa, a wnioski są przyjmowane do 30 października 2026 r. Katalog wydatków obejmuje sprzęt i oprogramowanie do ochrony sieci, licencje i usługi bezpieczeństwa, szkolenia pracowników oraz audyty i wdrożenie zabezpieczeń [26]. O kwalifikowalności systemu MDM rozstrzyga dokumentacja naboru. Warunki naboru, w tym wymóg partnerstwa i pułapy dofinansowania zależne od liczby jednostek, omawia artykuł CyberKatalog.pl o naborze LCC [27].

Rozdział 7

Wdrożenie i obsługa incydentów

7.1 Pilotaż

NIST zaleca wdrożenie pilotażowe i jego przetestowanie przed uruchomieniem rozwiązania produkcyjnie, a w fazie wdrożenia rozróżnia testy weryfikacyjne, sprawdzające, czy konfiguracja działa zgodnie z założeniami, od testów wdrożeniowych, sprawdzających zachowanie systemu w docelowym środowisku (5.3.5, 5.3.6) [2]. W urzędzie pilotaż obejmuje zwykle jedną komórkę organizacyjną i dział informatyki. Powinien sprawdzić techniczną rejestrację i procedury: wydanie urządzenia, zgłoszenie utraty, zmianę użytkownika i wycofanie. Każda z tych procedur powinna zostać przećwiczona co najmniej raz, zanim system obejmie cały urząd.

7.2 Ochrona konsoli

Konsola systemu MDM pozwala zablokować albo wymazać każde urządzenie w urzędzie jednym poleceniem. NIST wymienia kradzież danych logowania administratora EMM i zagrożenie wewnętrzne jako odrębne zagrożenia (3.2.2, 3.2.3) i zaleca stosowanie wobec infrastruktury zarządzania tych samych praktyk bezpieczeństwa co wobec innych systemów IT: zarządzania poprawkami, konfiguracją, tożsamością i dostępem (4.3.2) [2]. W praktyce urzędu oznacza to:

- uwierzytelnianie wieloskładnikowe dla każdego konta w konsoli;
- imienne konta administratorów, bez kont współdzielonych, także po stronie wykonawcy;
- role o ograniczonym zakresie: osoba obsługująca wydawanie urządzeń nie potrzebuje uprawnienia do zmiany polityk ani do pełnego wymazania;
- zatwierdzanie operacji masowych i pełnego wymazania przez drugą osobę, jeżeli system to umożliwia;
- przekazywanie dziennika działań w konsoli do systemu zbierania logów urzędu i przechowywanie go przez okres wymagany w KRI (§ 20 ust. 4) [16].

7.3 Utrata lub kradzież urządzenia

Utrata urządzenia jest zdarzeniem, dla którego procedurę można przygotować w całości z góry. Procedura powinna określać:

1. kanał zgłoszenia dostępny także poza godzinami pracy urzędu i bez użycia utraconego urządzenia;
2. kolejność działań: zablokowanie urządzenia, odebranie dostępu na koncie użytkownika, decyzja o wymazaniu;
3. kryteria decyzji o wymazaniu i osobę, która ją podejmuje;
4. zapis zdarzenia w rejestrze incydentów;
5. ocenę, czy zdarzenie jest naruszeniem ochrony danych osobowych, dokonywaną z udziałem inspektora ochrony danych.

Ocena z punktu 5 decyduje o obowiązku zgłoszenia naruszenia Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości w ciągu 72 godzin od jego stwierdzenia (art. 33 ust. 1 RODO), i o ewentualnym zawiadomieniu osób, których dane dotyczą (art. 34) [19]. Zawiadomienia osób nie wymaga się, jeżeli dane na utraconym urządzeniu były zaszyfrowane w sposób uniemożliwiający odczyt osobom nieuprawnionym (art. 34 ust. 3 lit. a). Fakty, które pozwalają ocenić ryzyko, pochodzą z systemu MDM: czy urządzenie było zaszyfrowane, czy miało blokadę ekranu, kiedy ostatnio łączyło się z serwerem i czy polecenie wymazania zostało wykonane. Bez systemu MDM urząd zna te fakty wyłącznie z deklaracji pracownika.

7.4 Incydenty w rozumieniu ustawy o KSC

Terminy zgłoszeń zależą od statusu jednostki. Podmiot kluczowy przekazuje właściwemu zespołowi CSIRT (art. 11 ust. 1 pkt 4-4c ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym nowelizacją):

- wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia;
- zgłoszenie incydentu poważnego niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia;
- na wniosek CSIRT sprawozdanie okresowe z obsługi incydentu poważnego;
- sprawozdanie końcowe nie później niż w ciągu miesiąca od dnia zgłoszenia incydentu poważnego.

Podmiot ważny będący podmiotem publicznym, na przykład urząd gminy poniżej progu zatrudnienia albo szkoła, zgłasza incydent poważny w tym samym terminie 72 godzin. Nie przekazuje wczesnego ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu obsługi incydentu ani sprawozdania końcowego (art. 12c). Zgłoszenia przekazuje się przez system teleinformatyczny z art. 46 ust. 1. Do czasu komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej trafiają one do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV (art. 44 ust. 1 ustawy nowelizującej). Jeżeli obowiązki z art. 11 wykonuje za jednostkę inna jednostka na podstawie art. 16e, zgłoszenia w imieniu podmiotu publicznego przekazuje jednostka wyznaczona (art. 16h pkt 1) [11]. Utrata pojedynczego zaszyfrowanego telefonu zwykle nie będzie incydentem poważnym. Przejęcie konsoli MDM albo złośliwe

oprogramowanie na wielu urządzeniach urzędu może nim być. Procedura obsługi incydentów urzędu powinna więc obejmować system MDM jako źródło informacji i jako możliwy cel ataku.

KRI niezależnie od statusu jednostki wymaga bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób (§ 19 ust. 2 pkt 13) [16]. Zgłoszenia między pracownikiem, działem informatyki, inspektorem ochrony danych i jednostką obsługującą, jeżeli urząd z niej korzysta, powinny przebiegać tą samą drogą bez względu na to, który z trzech reżimów prawnych w danym przypadku rozstrzyga.

7.5 Przegląd i audyt

KRI wymaga audytu wewnętrznego bezpieczeństwa informacji nie rzadziej niż raz na rok (§ 19 ust. 2 pkt 14) [16]. Podmiot kluczowy przeprowadza ponadto audyt bezpieczeństwa co najmniej raz na 3 lata, pierwszy w terminie 24 miesięcy od wejścia w życie nowelizacji (art. 15 ust. 1 ustawy o KSC i art. 33 ust. 2 ustawy nowelizującej). Podmiotowi ważnemu organ może nakazać audyt zewnętrzny po incydencie poważnym albo innym naruszeniu ustawy (art. 15 ust. 1b). Audytu nie może przeprowadzić osoba, która realizuje w audytowanym podmiocie zadania z art. 8 i art. 9-13 albo realizowała je w ciągu roku przed audytem (art. 15 ust. 2a) [11]. NIST zaleca, by okresowe audyty obejmowały system zarządzania urządzeniami, jego integracje i same urządzenia wraz z aplikacjami. Ich wyniki mają pozwolić ocenić, czy korzyści z dostępu mobilnego przewyższają ryzyko (5.4.1) [2]. Dane z systemu MDM ułatwiają taki audyt, bo raport zgodności z polityką pokazuje stan wszystkich urządzeń na dany dzień.

Załącznik A

Lista kontrolna

Lista porządkuje działania z rozdziałów 3-7. Nawias wskazuje rozdział albo podstawę.

Przed wdrożeniem

- ☐ Ustalono status urzędu i jednostek podległych w ustawie o KSC oraz sprawdzono zawiadomienie o wpisie do wykazu z urzędu; brakujące dane uzupełniono w terminie z wezwania ministra (KSC art. 7a ust. 2 pkt 3, art. 7b; rozdz. 3).
- ☐ Sprawdzono, czy urząd korzysta ze wspólnej obsługi albo porozumienia z art. 16e ustawy o KSC.
- ☐ Zinwentaryzowano urządzenia mające dostęp do danych urzędu, w tym prywatne z pocztą służbową (rozdz. 4).
- ☐ Sklasyfikowano informacje i przypisano im dopuszczalne modele urządzeń (rozdz. 5).
- ☐ Wybrano model własności dla każdej grupy stanowisk (rozdz. 2).
- ☐ Przeanalizowano obowiązek oceny skutków dla ochrony danych, zwłaszcza przy funkcji lokalizacji i urządzeniach prywatnych (RODO art. 35).
- ☐ Przetwarzanie danych w systemie MDM wpisano do rejestru czynności przetwarzania, a pracownikom przekazano informacje o przetwarzaniu (RODO art. 30 i 13).
- ☐ Przyjęto politykę urządzeń mobilnych z zakresem zarządzania (rozdz. 5).
- ☐ Cele, zakres i sposób monitoringu wpisano do regulaminu pracy uzgodnionego z zakładową organizacją związkową, pracowników uprzedzono co najmniej 2 tygodnie przed uruchomieniem, a nowym pracownikom przekazuje się te informacje na piśmie przed dopuszczeniem do pracy (KP art. 22^2 § 6-8 w zw. z art. 22^3 § 3, art. 104^2 § 1).
- ☐ Kierownik jednostki przeszedł w tym roku szkolenie z cyberbezpieczeństwa (KSC art. 8e ust. 1), a urząd ocenił, czy administratorzy MDM przedstawiają informację z Krajowego Rejestru Karnego o niekaralności za przestępstwa przeciwko ochronie informacji (KSC art. 8f ust. 1).
- ☐ Konta urzędu w programach rejestracji urządzeń twórców systemów operacyjnych należą do urzędu.

Zakup

- ☐ Ustalono wartość zamówienia jako całkowite szacunkowe wynagrodzenie wykonawcy bez VAT za cały okres umowy (Pzp art. 28 i 29).
- ☐ Sprawdzono decyzje o uznaniu za dostawcę wysokiego ryzyka ogłoszone w Monitorze Polskim i rekomendacje z art. 33 ust. 4 ustawy o KSC (KSC art. 67c, Pzp art. 226 ust. 1 pkt 17 i 19).
- ☐ Opis przedmiotu zamówienia jest funkcjonalny i nie wskazuje znaków towarowych (Pzp art. 99 ust. 4).
- ☐ Opis uwzględnia wymagania dostępności (Pzp art. 100 ust. 1).
- ☐ Projekt umowy powierzenia przetwarzania danych jest częścią dokumentacji (RODO art. 28 ust. 3).
- ☐ Umowa przewiduje eksport inwentarza i konfiguracji po jej zakończeniu.

Wdrożenie

- ☐ Konta administratorów są imienne i chronione uwierzytelnianiem wieloskładnikowym.
- ☐ Dziennik działań w konsoli trafia do systemu zbierania logów i jest przechowywany przez okres z przepisów odrębnych, a bez nich przez 2 lata (KRI § 20 ust. 4).
- ☐ Pilotaż objął wydanie urządzenia, utratę, zmianę użytkownika i wycofanie (rozdz. 7).
- ☐ Użytkownicy przeszli szkolenie (KRI § 19 ust. 2 pkt 6).

Wycofanie urządzenia

- ☐ Odebrano dostęp do zasobów urzędu na koncie użytkownika.
- ☐ Szyfrowanie było włączone przez cały okres użytkowania (raport z systemu MDM).
- ☐ Przywrócono ustawienia fabryczne i potwierdzono wykonanie w konsoli.
- ☐ Wyjęto i zniszczono kartę SIM i kartę pamięci (NIST 5.5).
- ☐ Sprawdzono, czy klucz szyfrowania nie ma kopii poza urządzeniem.
- ☐ Sporządzono protokół z identyfikatorem z inwentarza, datą, sposobem, osobą wykonującą i zatwierdzającą.
- ☐ Zaktualizowano inwentarz.

Załącznik B

Struktura polityki urządzeń mobilnych

Poniższa struktura jest punktem wyjścia do zarządzenia kierownika jednostki. Nie jest gotowym tekstem: każdy punkt wymaga rozstrzygnięć właściwych dla urzędu, opisanych w rozdziale 5.

1. Cel i zakres: jednostki objęte polityką, w tym jednostki obsługiwane albo objęte porozumieniem; rodzaje urządzeń; relacja do dokumentacji systemu zarządzania bezpieczeństwem informacji.
2. Definicje: każdy użyty skrót (MDM, MAM, BYOD, CYOD, COPE), z definicją przyjętą w urzędzie.
3. Role: kierownik jednostki, administrator systemu, inspektor ochrony danych, osoba odpowiedzialna za cyberbezpieczeństwo, użytkownik, wykonawca.
4. Klasyfikacja informacji i dopuszczalne modele urządzeń: tabela z kolumnami grupa informacji, dopuszczalny model, wymagane zabezpieczenia.
5. Wymagania wobec urządzeń: wspierana wersja systemu, blokada ekranu, szyfrowanie, źródła aplikacji, stan zabezpieczeń producenta.
6. Zakres zarządzania: funkcje systemu MDM stosowane i wyłączone, oddzielnie dla urządzeń służbowych i prywatnych; wskazanie funkcji będących inną formą monitoringu, których cele, zakres i sposób przenosi się do regulaminu pracy (art. 22^2 § 6 KP).
7. Cykl życia urządzenia: wydanie, zmiana użytkownika, zwrot, wycofanie, protokoły.
8. Urządzenia prywatne: warunki dopuszczenia, zakres danych służbowych, wymazanie selektywne, zasady ekwiwalentu przy pracy zdalnej.
9. Utrata, kradzież i incydenty: kanał zgłoszenia, kolejność działań, rola inspektora ochrony danych, powiązanie z procedurą obsługi incydentów.
10. Administracja systemem: konta imienne, uwierzytelnianie wieloskładnikowe, role, zatwierdzanie operacji krytycznych, dziennik działań.
11. Szkolenia: zakres i częstotliwość.
12. Przegląd: termin przeglądu polityki, co najmniej przy audycie wewnętrznym.

Załącznik C

Kryteria do opisu przedmiotu zamówienia

Tabela C.1 zawiera wymagania, z których urząd może ułożyć opis przedmiotu zamówienia na system MDM. Nie jest kompletna ani obowiązkowa. Wymagania oznaczone jako podstawowe mają oparcie w przepisach, w zaleceniach NIST albo w ustaleniach rozdziałów poradnika i są właściwe dla każdego urzędu; pozostałe zależą od modelu własności, sposobu obsługi i środowiska urzędu. Kolumna "Związek" wskazuje przepis, zalecenie albo rozdział poradnika, z którego wymaganie wynika.

Tabela C.1: Kryteria funkcjonalne systemu MDM

Wymaganie	Rodzaj	Związek
Obsługa platform mobilnych wskazanych przez zamawiającego, w wersjach wspieranych przez ich twórców	podstawowe	KRI § 19 ust. 2 pkt 12 lit. a
Rejestracja urządzeń w programach rejestracji automatycznej twórców systemów operacyjnych, z kontami należącymi do zamawiającego	podstawowe	rozdz. 2
Inwentarz obejmujący model, numer seryjny, wersję systemu, stan szyfrowania, zainstalowane aplikacje zarządzane i użytkownika, z eksportem do formatu otwartego	podstawowe	KRI § 19 ust. 2 pkt 2; KSC art. 8 ust. 1 pkt 2 lit. m
Wymuszanie blokady ekranu, złożoności kodu i czasu automatycznej blokady	podstawowe	RODO art. 32
Wymuszanie i raportowanie szyfrowania pamięci	podstawowe	RODO art. 32 ust. 1 lit. a; KSC art. 8 ust. 1 pkt 2 lit. k
Zdalne zablokowanie, wymazanie pełne i wymazanie wyłącznie danych służbowych	podstawowe	RODO art. 5 ust. 1 lit. f

Wymaganie	Rodzaj	Związek
Raport zgodności urządzeń z polityką i alert przy niezgodności	podstawowe	RODO art. 24 ust. 1
Ograniczenie dostępu do zasobów zamawiającego dla urządzeń niezgodnych z polityką	podstawowe	NIST 4.2.1.1
Dystrybucja i usuwanie aplikacji służbowych, lista aplikacji dozwolonych	podstawowe	NIST 4.2.2
Zarządzanie aplikacjami i danymi służbowymi na urządzeniach prywatnych bez zarządzania całym urządzeniem	zależne od modelu	rozdz. 5
Możliwość wyłączenia lokalizacji i odczytu aplikacji prywatnych w polityce	zależne od modelu	KP art. 22^3
Konfiguracja poczty, sieci bezprzewodowej i VPN przez profile	zależne od środowiska	NIST 4.2.1.3
Integracja z katalogiem tożsamości zamawiającego	zależne od środowiska	KRI § 19 ust. 2 pkt 5
Uwierzytelnianie wieloskładnikowe i role administratorów o ograniczonym zakresie	podstawowe	NIST 3.2.2, 4.3.2; KSC art. 8 ust. 1 pkt 2 lit. l
Dziennik działań administratorów z eksportem do systemu zbierania logów	podstawowe	KRI § 20
Rozdzielenie urządzeń i uprawnień administratorów według jednostek organizacyjnych	zależne od modelu obsługi	ustawa o KSC art. 16e
Przetwarzanie danych w EOG albo z zabezpieczeniami przewidzianymi w RODO	podstawowe	RODO art. 28 ust. 3 lit. a, rozdz. V
Oferowane produkty ICT nie są objęte decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka ani rekomendacją z art. 33 ust. 4 KSC	podstawowe	KSC art. 67c; Pzp art. 226 ust. 1 pkt 17 i 19
Dostępność konsoli i aplikacji dla osób z niepełnosprawnościami	podstawowe	Pzp art. 100 ust. 1
Eksport konfiguracji i inwentarza przy zakończeniu umowy	podstawowe	rozdz. 6

Bibliografia

[1] Główny Urząd Statystyczny. *Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2025 r.* 18 maja 2026. URL: https://web.archive.org/web/20260919080434/https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-w-2025-r-,7,8.html (dostęp 19 września 2026).

[2] Gema Howell, Joshua M. Franklin, Vincent Sritapan, Murugiah Souppaya i Karen Scarfone. *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* NIST Special Publication 800-124 Rev. 2. National Institute of Standards and Technology, maj 2023. DOI: 10.6028/NIST.SP.800-124r2. URL: https://web.archive.org/web/20260919080855/https://csrc.nist.gov/pubs/sp/800/124/r2/final (dostęp 19 września 2026).

[3] CyberKatalog.pl. *MDM (Mobile Device Management).* Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/mdm (dostęp 19 września 2026).

[4] Silesian Solutions. *MDM w jednostkach samorządu terytorialnego: co mówi prawo.* 19 września 2026. URL: https://silesiansolutions.com/blog/mdm-w-jednostkach-samorzadu-terytorialnego/ (dostęp 19 września 2026).

[5] CyberKatalog.pl. *MAM (Mobile Application Management).* Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/mam (dostęp 19 września 2026).

[6] CyberKatalog.pl. *EMM (Enterprise Mobility Management).* Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/emm (dostęp 19 września 2026).

[7] CyberKatalog.pl. *UEM (Unified Endpoint Management).* Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/uem (dostęp 19 września 2026).

[8] CyberKatalog.pl. *COPE (Corporate-Owned, Personally Enabled).* Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/cope (dostęp 19 września 2026).

[9] CyberKatalog.pl. *BYOD (Bring Your Own Device).* Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/byod (dostęp 19 września 2026).

[10] CyberKatalog.pl. *CYOD (Choose Your Own Device)*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/cyod (dostęp 19 września 2026).

[11] *Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*. Dz.U. 2026 poz. 252. 2 marca 2026. URL: https://dziennikustaw.gov.pl/DU/2026/252 (dostęp 19 września 2026).

[12] *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 (dyrektywa NIS 2)*. Dz.Urz. UE L 333 z 27.12.2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/pol (dostęp 19 września 2026).

[13] CyberKatalog.pl. *NIS2*. Hasło w słowniku cyberbezpieczeństwa. URL: https://cyberkatalog.pl/slownik/nis2 (dostęp 19 września 2026).

[14] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*. Dz.U. 2018 poz. 1560. URL: https://dziennikustaw.gov.pl/DU/2018/1560 (dostęp 19 września 2026).

[15] Minister Cyfryzacji. *Komunikat Ministra Cyfryzacji z dnia 8 kwietnia 2026 r. w sprawie harmonogramu złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych oraz rozpoczęcia korzystania z systemu teleinformatycznego przez podmioty kluczowe lub podmioty ważne*. Dz. Urz. Min. Cyfr. 2026 poz. 7. 8 kwietnia 2026. URL: https://web.archive.org/web/20260501125526/https://www.gov.pl/attachment/a3b63395-503b-426c-9913-6d0b6d3c205d (dostęp 19 września 2026).

[16] *Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*. Dz.U. 2024 poz. 773. 22 maja 2024. URL: https://dziennikustaw.gov.pl/DU/2024/773 (dostęp 19 września 2026).

[17] *Ustawa z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw*. Dz.U. 2025 poz. 1158. 22 sierpnia 2025. URL: https://dziennikustaw.gov.pl/DU/2025/1158 (dostęp 19 września 2026).

[18] Kancelaria Sejmu. *Internetowy System Aktów Prawnych, metryka aktu Dz.U. 2024 poz. 773*. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240000773 (dostęp 19 września 2026).

[19] *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 (RODO)*. Dz.Urz. UE L 119 z 4.5.2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/pol (dostęp 19 września 2026).

[20] Prezes Urzędu Ochrony Danych Osobowych. *Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony*. M.P.

2019 poz. 666. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190000666 (dostęp 19 września 2026).

[21] *Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy, tekst jednolity.* Dz.U. 2025 poz. 277 ze zm. URL: https://dziennikustaw.gov.pl/DU/2025/277 (dostęp 19 września 2026).

[22] *Rozporządzenie Komisji (UE) 2023/1670 z dnia 16 czerwca 2023 r. ustanawiające wymogi dotyczące ekoprojektu dla smartfonów, telefonów komórkowych innych niż smartfony, telefonów bezprzewodowych i komputerów typu slate na podstawie dyrektywy Parlamentu Europejskiego i Rady 2009/125/WE oraz zmieniające rozporządzenie Komisji (UE) 2023/826.* Dz.Urz. UE L 214 z 31.8.2023, z późn. zm. URL: https://eur-lex.europa.eu/eli/reg/2023/1670/oj/pol (dostęp 19 września 2026).

[23] *Ustawa z dnia 11 września 2019 r. - Prawo zamówień publicznych, tekst jednolity.* Dz.U. 2026 poz. 793. URL: https://dziennikustaw.gov.pl/DU/2026/793 (dostęp 19 września 2026).

[24] Prezes Urzędu Zamówień Publicznych. *Obwieszczenie Prezesa Urzędu Zamówień Publicznych z dnia 8 grudnia 2025 r. w sprawie aktualnych progów unijnych, ich równowartości w złotych, równowartości w złotych kwot wyrażonych w euro oraz średniego kursu złotego w stosunku do euro stanowiącego podstawę przeliczania wartości zamówień publicznych lub konkursów.* M.P. 2025 poz. 1247. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20250001247 (dostęp 19 września 2026).

[25] Centrum Projektów Polska Cyfrowa. *Cyberbezpieczny Samorząd: więcej czasu na realizację grantu.* 16 czerwca 2026. URL: https://web.archive.org/web/20260902163532/https://www.gov.pl/web/cppc/aktualizacja-dokumentacji-cyberbezpieczny-samorzad-16062026 (dostęp 19 września 2026).

[26] Centrum Projektów Polska Cyfrowa. *Samorządy wspólnie ochronią swoje systemy przed cyberatakami.* 31 lipca 2026. URL: https://web.archive.org/web/20260902162244/https://www.gov.pl/web/cppc/uruchomienie-naboru-FERC0401IP0100326 (dostęp 19 września 2026).

[27] CyberKatalog.pl. *Lokalne Centra Cyberbezpieczeństwa: nabór LCC do 30 października.* 2 września 2026. URL: https://cyberkatalog.pl/aktualnosci/artykuly/lokalne-centra-cyberbezpieczenstwa-nabor-lcc-2026 (dostęp 19 września 2026).