KLASTER
INNOWACJI
SPOŁECZNYCH

CYFROWY URZĘDNIK

Praktyczny przewodnik kompetencji cyfrowych

Podręcznik uczestnika
14-godzinnego cyklu szkoleniowego (Blok I + Blok II)

Projekt: „Uzupełnienie umiejętności cyfrowych pracowników JST i zwiększenie wykorzystania narzędzi technologii informacyjno-komunikacyjnej w województwie śląskim”

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
CENTRUM PROJEKTÓW POLSKA CYFROWA
KLASTER INNOWACJI SPOŁECZNYCH
NEW EUROPE FOUNDATION
INSTYTUT ROŻDZIEŃSKIEGO

“

Tytuł: Cyfrowy urzędnik. Praktyczny przewodnik kompetencji cyfrowych.

Projekt: „Uzupełnienie umiejętności cyfrowych pracowników JST i zwiększenie wykorzystania narzędzi technologii informacyjno-komunikacyjnej w województwie śląskim”.

Numer projektu: KPOD.05.08-IW.06-0089/25-00.

Finansowanie: Publikacja sfinansowana ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Inwestycja C2.1.3 „E-kompetencje”. Instrument: NextGenerationEU. Jednostka wspierająca: Centrum Projektów Polska Cyfrowa (CPPC).

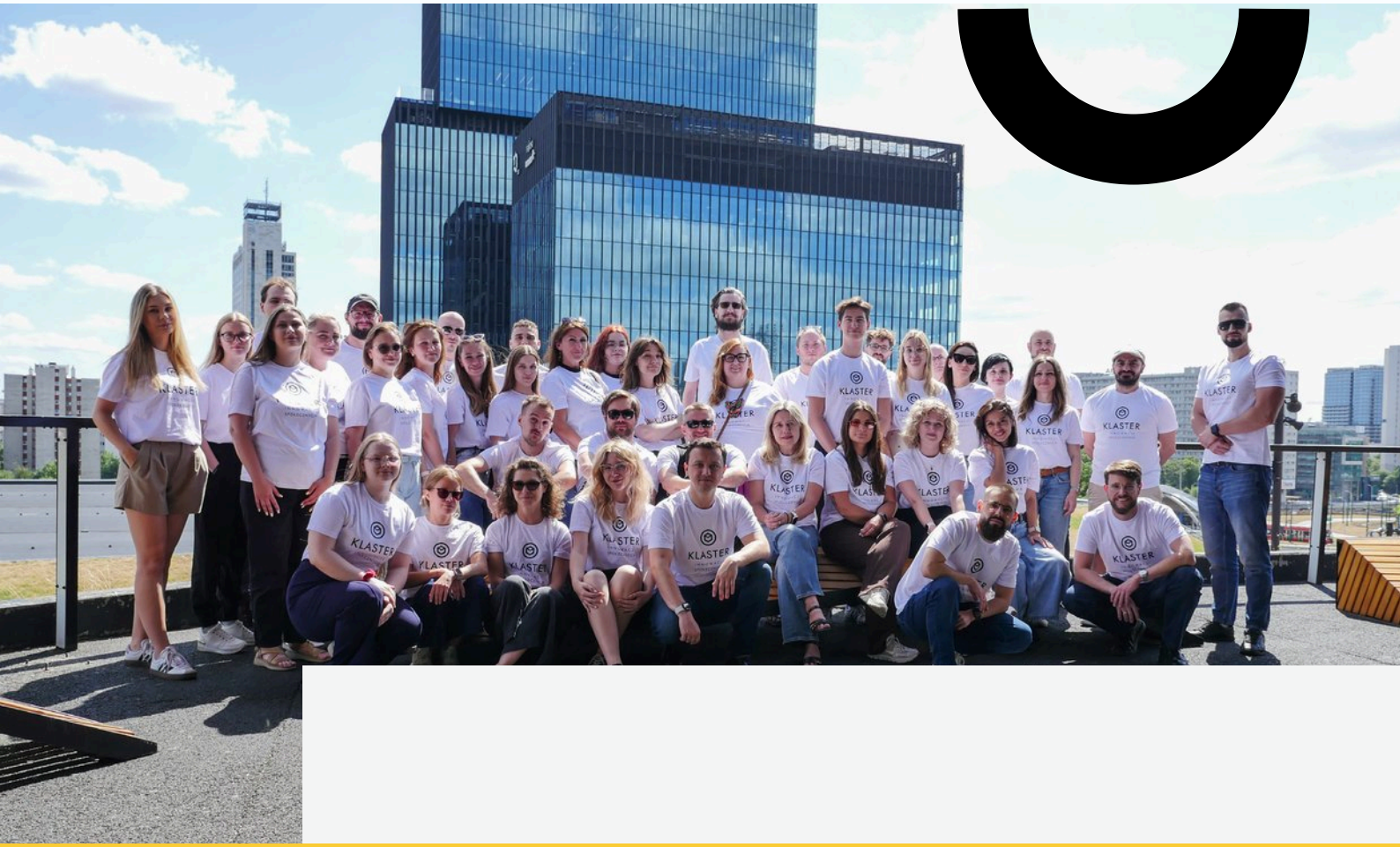
Realizatorzy: Fundacja Klaster Innowacji Społecznych (KIS) · New Europe Foundation (NEF) · Instytut Rozdzieńskiego (IR).

Opracowanie merytoryczne: zespół ekspertów i praktyków projektu UUCPJST pod redakcją Roberta Kłosowskiego.

Weryfikacja merytoryczna: ekspert ds. kompetencji cyfrowych.

Wydanie I, Gliwice 2026

Spis treści



Fundacja Klaster Innowacji Społecznych

O nas

Ten podręcznik powstał dzięki współpracy trzech śląskich organizacji pozarządowych, które od lat łączy jedno przekonanie. Nowoczesne technologie mają służyć człowiekowi, a nie go onieśmielać. Każda z nas wnosi do projektu własne doświadczenie, od cyfrowej edukacji, przez pracę u podstaw ze społecznościami, po wieloletnią praktykę w prowadzeniu projektów. Razem tworzymy zespół, który wie, jak zamienić wiedzę w konkretne, przydatne umiejętności.

KLASTER INNOWACJI SPOŁECZNYCH

Fundacja Klaster Innowacji Społecznych

jest liderem projektu i pomysłodawcą tej książki. Działamy z Gliwic od 2015 roku, stojąc na czele konsorcjum dziewięciu śląskich organizacji i przedsiębiorstw społecznych. W naszym dorobku jest już ponad dwieście inicjatyw, a przeszło sto czterdzieści z nich zdążyliśmy zrealizować i rozliczyć. Naszą codziennością jest przekładanie sztucznej inteligencji, cyfryzacji i funduszy zewnętrznych na realne kompetencje ludzi oraz instytucji. O technologii nie tylko uczymy. Sami pracujemy na własnym systemie CRM, korzystamy z narzędzi opartych na AI i udostępniamy organizacjom pozarządowym bezpłatną bramkę sztucznej inteligencji. Ten praktyczny, sprawdzony we własnej pracy charakter chcieliśmy przenieść na karty podręcznika. Pełny wykaz przydatnych aplikacji i stron znajdziesz w katalogu na końcu książki, a źródła oraz materiały dla grafika zebraliśmy w aneksie. Dobre praktyki opisane w tekście traktuj jak gotowe wskazówki do wdrożenia od jutra.

NEW EUROPE FOUNDATION

New Europe Foundation

jest partnerem projektu i częścią tego samego konsorcjum. To niezależna organizacja, która wspiera demokrację, społeczeństwo obywatelskie i współpracę w Europie Środkowej. Na co dzień prowadzi wymiany młodzieżowe i wolontariat w programie Erasmus+, projekty integracyjne dla migrantów oraz działania edukacyjne uczące krytycznego myślenia i odporności na dezinformację. Fundacja od lat buduje mosty między Śląskiem a partnerami z całej Europy i Partnerstwa Wschodniego, wnosząc do projektu międzynarodowe spojrzenie i wyczucie potrzeb bardzo różnych odbiorców.

Trzy organizacje, jeden cel.

INSTYTUT
ROŻDZIEŃSKIEGO

Instytut Rożdzieńskiego

odpowiada za realizację działań w projekcie. Ta katowicka organizacja wzięła nazwę od Walentego Rożdzieńskiego, śląskiego kuźnika i poety sprzed czterech wieków, i do dziś kuje coś równie trwałego, czyli aktywne i świadome społeczeństwo obywatelskie. Przez dekadę działalności zrealizowała blisko sto projektów krajowych i międzynarodowych, w których wzięło udział niemal trzynaście tysięcy osób. Instytut prowadzi Akademię Wolontariatu, debaty o przyszłości śląskich miast oraz programy poświęcone sprawiedliwej transformacji regionu, zawsze blisko mieszkańców i ich codziennych spraw.

Połączyły nas wspólne wartości i jeden cel. Chcemy, żeby cyfrowa administracja była bliższa człowiekowi, a praca urzędnika łatwiejsza, bezpieczniejsza i bardziej ludzka. Ten podręcznik jest tego dobrym początkiem.

Wstęp. Jak korzystać z podręcznika

Słowo od organizatora

Fundacja Klaster Innowacji Społecznych działa od 2015 roku i jest dziś jedną z najprężniejszych organizacji pozarządowych na południu Polski. Od początku stawiamy na edukację cyfrową. Zrealizowaliśmy blisko sto projektów, które dotarły do ponad piętnastu tysięcy osób. Prowadzimy Kluby Rozwoju Cyfrowego, szkolimy pracowników administracji i pomagamy lokalnym społecznościom oswajać nowe technologie, od cyberbezpieczeństwa po codzienne e-usługi.

Z urzędami pracujemy na co dzień, dlatego dobrze znamy realia tej pracy. Za każdą procedurą stoi konkretny człowiek, który chce sprawnie obsłużyć mieszkańca, a czasem brakuje mu czasu albo narzędzi, żeby nadążyć za zmianami. Z myślą o nim powstał ten podręcznik. Zebraliśmy w nim to, co naprawdę przydaje się w pracy, i opisaliśmy prostym językiem. Mamy nadzieję, że stanie się Twoim praktycznym towarzyszem, do którego nieraz wrócisz po szkoleniu.

O podręczniku

Trzymasz w rękach przewodnik, który powstał jako trwały efekt szkolenia w projekcie UUCPJST. Jego celem jest **utrwalenie** wiedzy zdobytej na zajęciach i **rozszerzenie** jej o praktyczne wskazówki, do których wrócisz w codziennej pracy.

To nie podręcznik akademicki. To **praktyczne kompendium** napisane z myślą o urzędniku, niezależnie od stanowiska i poziomu zaawansowania cyfrowego. Znajdziesz tu konkretne kroki, listy kontrolne i przykłady z polskiej administracji.

Jak korzystać z podręcznika

Rozdziały możesz czytać w dowolnej kolejności, bo każdy jest samodzielną całością. Każdy zaczyna się krótkim wprowadzeniem, a kończy blokiem „W skrócie" z najważniejszymi, praktycznymi wnioskami. Pełny wykaz przydatnych aplikacji i stron znajdziesz w katalogu na końcu książki, a źródła oraz materiały dla grafika zebraliśmy w aneksie. Dobre praktyki opisane w tekście traktuj jak gotowe wskazówki do wdrożenia od jutra.

Symbol	Znaczenie
Dobra praktyka	Konkretna wskazówka do natychmiastowego zastosowania.
Uwaga / Ryzyko	Częsty błąd lub zagrożenie do uniknięcia.
Przykład z urzędu	Krótki, realny kontekst z administracji.
W skrócie	Najważniejsze wnioski na końcu każdego rozdziału.

Wprowadzenie. Dlaczego kompetencje cyfrowe w urzędzie

Cyfryzacja administracji to nie moda, lecz codzienność. Mieszkańcy coraz częściej załatwiają sprawy online, przepisy wymagają dostępności i bezpieczeństwa danych, a nowe narzędzia, od e-Doręczeń po sztuczną inteligencję, zmieniają sposób pracy urzędu.

Kompetencje cyfrowe urzędnika przekładają się wprost na codzienną pracę. Pierwsza korzyść to lepsza obsługa mieszkańca: szybciej, wygodniej i bez zbędnych wizyt. Druga to bezpieczeństwo, rozumiane jako ochrona danych i odporność na cyberzagrożenia. Rośnie też efektywność, bo mniej papieru i mniej błędów oznacza więcej czasu na sprawy naprawdę ważne. Liczy się wreszcie równość, czyli dostępność usług dla wszystkich, w tym osób ze szczególnymi potrzebami.

Ten podręcznik prowadzi przez **dwa bloki tematyczne** 14-godzinnego cyklu szkoleniowego.

Mapa cyklu szkoleniowego
Blok I - kompetencje horyzontalne (wspólne dla każdego urzędnika, niezależnie od stanowiska):
1. Dostępność cyfrowa dokumentów
2. Cyberbezpieczeństwo i ochrona danych
3. Zarządzanie danymi i otwieranie danych
4. Odporność i higiena cyfrowa
5. Aplikacje krajowe i e-administracja
6. Komunikacja w pracy zdalnej
Blok II - kompetencje specjalistyczne (praktyka pod konkretne zadania):
7. AI w pracy urzędnika - od teorii do praktyki
8. Obsługa mieszkańców w środowisku cyfrowym
9. Case studies, czyli cyfryzacja w praktyce

Każdy rozdział tego podręcznika odpowiada jednemu modułowi szkolenia. Możesz czytać po kolei albo sięgać po temat, którego akurat potrzebujesz.

Wskazówka. Jeśli nie wiesz, od czego zacząć, przejdź Blok I po kolei.
To fundament, na którym opierają się kompetencje specjalistyczne z Bloku II.

Rozdział 1. Dostępność cyfrowa dokumentów

Ten rozdział wyjaśnia, czym jest dostępność cyfrowa, dlaczego jest Twoim obowiązkiem prawnym i jak tworzyć dostępne pisma, korzystając z czterech zasad standardu WCAG oraz prostego języka.

Czym jest dostępność cyfrowa

Dostępność cyfrowa to projektowanie treści i usług online tak, aby mógł z nich skorzystać każdy, niezależnie od wzroku, słuchu, sprawności ruchowej czy poziomu cyfrowych umiejętności. Dostępny dokument można przeczytać, zrozumieć i obsłużyć również za pomocą czytnika ekranu, samej klawiatury albo na małym ekranie telefonu. To nie jest dodatek dla wybranych, bo z dostępności korzystają wszyscy: osoba z niepełnosprawnością wzroku, senior, mieszkaniec czytający pismo w pośpiechu na telefonie i urzędnik, który szybko szuka właściwego fragmentu.

🏛 **Decyzja administracyjna zapisana jako skan podpisanego papieru jest dla czytnika ekranu zwykłym obrazkiem i osoba niewidoma nie odczyta z niej ani słowa, podczas gdy ten sam dokument zapisany jako PDF z tekstem i strukturą jest w pełni dostępny.**

Dlaczego to ważne: prawo i liczby

Dla podmiotów publicznych dostępność cyfrowa jest obowiązkiem prawnym. Wynika z ustawy z dnia 4 kwietnia 2019 roku o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, która wymaga zgodności ze standardem WCAG na poziomie 2.1 AA[1]. Odrębnym aktem jest Europejski akt o dostępności (European Accessibility Act), obowiązujący od 28 czerwca 2025 roku. Adresowany jest przede wszystkim do podmiotów gospodarczych i obejmuje wybrane produkty oraz usługi rynkowe, takie jak e-usługi, bankowość czy e-commerce[2]. Dla urzędu EAA ma znaczenie głównie pośrednie, na przykład przy zamawianiu produktów i usług cyfrowych. Niezależnie od tego sprawdź, czy strony i e-usługi urzędu spełniają WCAG, i zaktualizuj deklarację dostępności oraz ścieżkę zgłaszania barier[2].

Przy okazji uporządkujmy nazewnictwo. Prawo, w tym norma EN 301 549, odwołuje się dziś do WCAG 2.1 AA, ale najnowsza wersja wytycznych to WCAG 2.2 i to ją przyjęliśmy jako standard dla samego podręcznika oraz materiałów projektu. Różnice między 2.1 a 2.2 to głównie dodatkowe kryteria ułatwień, na przykład większy rozmiar pól dotykowych. Idą tą drogą także inni: brytyjski rząd wskazał WCAG 2.2 AA jako nowy minimalny standard dostępności stron i aplikacji sektora publicznego, pokazując, że jego system projektowy gov.uk pomaga szybciej spełnić nowe kryteria, takie jak większe pola dotykowe i widoczny fokus[7]. To praktyczny argument, by w urzędzie projektować już pod WCAG 2.2, a nie tylko 2.1.

Za brak dostępności grożą kary. Grzywna wynosi do 10 000 złotych za stronę lub aplikację oraz do 5000 złotych za brak lub niepoprawną deklarację dostępności[1]. Skala potrzeb jest duża, bo około 16 procent (około 1,3 miliarda osób) populacji to osoby z niepełnosprawnościami, a znaczna część dorosłych Polaków ma trudności z rozumieniem standardowych dokumentów urzędowych[3].

16%

osoby z niepełnosprawnościami

4,5 mln

Polaków – trudności z czytaniem dokumentów”

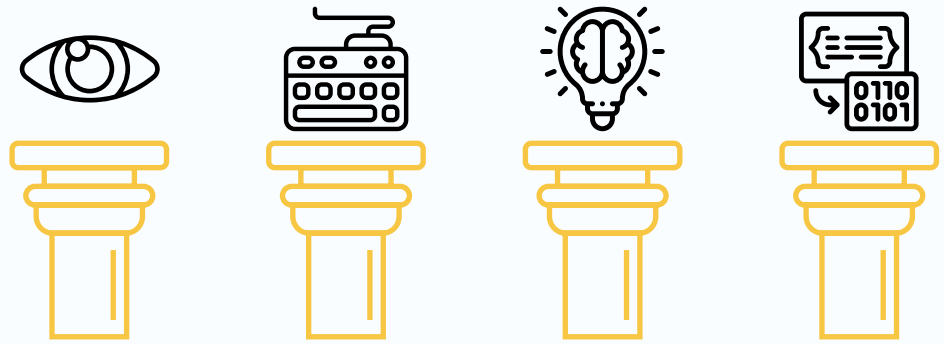
87%

urzędów – istotne bariery (NIK 2025)

🏛 Najwyższa Izba Kontroli sprawdziła dostępność w samorządach w latach 2019–2025 i wynik był jednoznaczny: żadna ze zbadanych stron internetowych urzędów nie spełniła wszystkich wymaganych kryteriów dostępności cyfrowej, a w ponad 87 procentach urzędów wykryto istotne bariery, także informacyjno-komunikacyjne[4]. To pokazuje, że dostępność wciąż wymaga codziennej uwagi każdego urzędnika.

Standard WCAG i cztery zasady P.O.U.R.

WCAG (Web Content Accessibility Guidelines) to międzynarodowy standard dostępności opracowany przez W3C[5]. Opiera się na czterech zasadach, w skrócie P.O.U.R. Postrzegalność oznacza, że informację da się odebrać różnymi zmysłami, dzięki tekstom alternatywnym do grafik, odpowiedniemu kontrastowi i napisom do filmów. Funkcjonalność to możliwość obsługi wszystkiego, na przykład samą klawiaturą, z dość długim czasem na działanie i bez treści wywołujących napady, takich jak miganie. Zrozumiałość wymaga prostego języka, przewidywalnego układu i pomocy w unikaniu błędów. Kompatybilność oznacza poprawną strukturę, czyli nagłówki i znaczniki, oraz zgodność z czytnikami ekranu.



Dostępny dokument krok po kroku

Punktem wyjścia jest kontrast. Tekst musi wyraźnie odcinać się od tła, a minimalny kontrast to 4,5 : 1 dla zwykłego tekstu oraz 3 : 1 dla dużego tekstu i elementów interfejsu. Nie używaj samego koloru do przekazania informacji, na przykład komunikatu, że pola na czerwono są obowiązkowe. Zawsze dodaj do tego etykietę lub symbol. Kontrast łatwo zweryfikować narzędziami WebAIM Contrast Checker lub WAVE.

Dokument buduj z nagłówków, gdzie Nagłówek 1 to tytuł, Nagłówek 2 to sekcja, a Nagłówek 3 to podsekcja. To one tworzą szkielet, po którym porusza się czytnik ekranu i z którego powstaje automatyczny spis treści. ⚠ Nie powiększaj zwykłego tekstu, aby udawał nagłówek, tylko używaj prawdziwych stylów nagłówków. Ważnych informacji nie umieszczaj też wyłącznie w nagłówku lub stopce dokumentu Word, bo łatwo je tam przeoczyć[3].

W typografii stosuj kroje bezszeryfowe, bo są czytelniejsze na ekranie, i wybieraj taki, w którym łatwo odróżnić podobne znaki, na przykład małe „l" od wielkiego „I", a połączenie „rn" od „m"[3]. Unikaj długich fragmentów kursywą i kapitalikami, a do wyróżnień używaj pogrubienia lub większego stopnia pisma, a nie samego koloru. Nie justuj tekstu, czyli nie wyrównuj go do obu marginesów naraz, bo nierówne odstępy między wyrazami utrudniają czytanie osobom z dysleksją i słabowidzącym[3].

Każda grafika niosąca treść potrzebuje krótkiego opisu alternatywnego (ALT), do około 125 znaków, który opisuje funkcję i znaczenie, a nie wygląd, i nie zaczyna się od słów „obraz" czy „zdjęcie". Grafika czysto dekoracyjna powinna mieć pusty opis (czyli zostaw pusty tekst alternatywny), a wykres lub tabela opis wraz z kluczowymi danymi. Zamiast pisać „wykres słupkowy", napisz: „Dochody gminy wzrosły z 5,2 mln zł w 2023 r. do 6,1 mln zł w 2024 r.".

Język pism musi być prosty i konkretny: zdania do około 20 słów, strona czynna, bez urzędowego żargonu, ze skrótami i skrótowcami wyjaśnianymi przy pierwszym użyciu[3]. Zrozumiałość polskiego tekstu pomaga zmierzyć narzędzie Jasnopis.pl. Zamiast „uiszczenie opłaty za gospodarowanie odpadami komunalnymi" wystarczy „zapłata za wywóz śmieci", zamiast „Decyzja została wydana" lepiej brzmi „Wydaliśmy decyzję", a w miejsce „należy przedłożyć stosowne załączniki" napisz wprost „dołącz: kopię dowodu i zaświadczenie o zarobkach".

Prosty język to dziś standard w polskiej administracji. W 2018 roku instytucje publiczne podpisały deklarację prostego języka, ZUS prowadzi program „Prosto z ZUS", a poradniki dla urzędników wdrożyły między innymi Poznań i Warszawa[6]. Można też korzystać z gotowych szkoleń, bo Krajowa Szkoła Administracji Publicznej wspólnie z Pracownią Prostej Polszczyzny Uniwersytetu Wrocławskiego prowadzi bezpłatne webinaria pod patronatem Szefa Służby Cywilnej, między innymi o tym, jak przygotować pismo urzędowe do uproszczenia[8]. Dobrym wzorem jest też podejście brytyjskiego Ministerstwa Edukacji, które oparty na normie ISO standard prostego języka sprowadziło do trzech kroków: użytkownik ma znaleźć informację, zrozumieć ją i móc zadziałać; urząd może przyjąć podobny, krótki standard wewnętrzny zamiast luźnych zaleceń[9].

zdanie urzędowe	prosty język
opłata za odpady	**wywóz śmieci**
decyzja została wydana	**wydaliśmy decyzję**
przedłożyć załączniki	**dołącz kopię dowodu i zaświadczenie**

Listy twórz z wbudowanych stylów, a nie z ręcznych myślników, używając numeracji, gdy ważna jest kolejność lub kroki, i wypunktowania, gdy elementy są równorzędne. Spis treści generuj automatycznie z nagłówków, w MS Word przez Odwołania i Spis treści. Jeśli zbierasz dane od mieszkańców, twórz formularze w formacie HTML zamiast .docx, bo są dostępniejsze i wygodniejsze do wypełnienia[3]. Pliki nazywaj według jednego schematu Temat_Wersja_Status_Data, na przykład Regulamin_RODO_v1_FINAL_2026-06-30.docx, i unikaj nazw typu dokument1.docx czy nowy_final_kopia2.pdf.

Osiem najczęstszych błędów

W codziennej pracy powtarza się ten sam zestaw potknięć: zbyt niski kontrast tekstu, brak hierarchii nagłówków i tekst zapisany „na płasko", tabele bez wierszy lub kolumn nagłówkowych, kolor jako jedyny nośnik informacji, brak tekstów alternatywnych do grafik, skomplikowany urzędowy język, listy robione myślnikami zamiast stylem listy oraz PDF-y bez struktury, czyli skany zamiast tekstu z tagami.

Zanim wyślesz dokument, włącz w Wordzie funkcję Sprawdź dostępność (Recenzja, a następnie Sprawdź dostępność), bo wskaże ona większość powyższych błędów. Pomocny jest też szybki test odczytu czytnikiem Windows Narrator (Win + Ctrl + Enter), a oficjalne dobre praktyki i przykłady deklaracji znajdziesz na gov.pl/web/dostępność-cyfrowa. Najlepszą zasadą pozostaje projektowanie dostępności od początku, a nie na końcu, gdy zabraknie już czasu, oraz zapewnianie różnych form kontaktu z urzędem, takich jak e-mail, telefon i polski język migowy, wraz z transkrypcjami do nagrań wideo[3].

W skrócie. *Dostępność cyfrowa jest obowiązkiem prawnym wynikającym z ustawy z 2019 roku (Europejski akt o dostępności to odrębny reżim dla sektora prywatnego), a za jej brak grożą kary do 10 000 złotych. Pisz dostępnie od początku: zadbaj o kontrast co najmniej 4,5 : 1, prawdziwe style nagłówków, opisy alternatywne grafik i prosty język z krótkimi zdaniami. Nie polegaj wyłącznie na kolorze, nie justuj tekstu i nie wysyłaj decyzji jako skanu bez warstwy tekstowej. Przed publikacją uruchom w Wordzie funkcję Sprawdź dostępność i popraw zgłoszone błędy. Projektuj już pod WCAG 2.2, bo to kierunek, w którym idzie cały sektor publiczny.*

Rozdział 2. Cyberbezpieczeństwo i ochrona danych

Ten rozdział pokazuje, jak rozpoznawać najczęstsze zagrożenia, tworzyć silne hasła i włączać uwierzytelnianie dwuskładnikowe, bezpiecznie wymieniać pliki oraz prawidłowo reagować na incydenty i zgłaszać je właściwym służbom.

Dlaczego to sprawa każdego urzędnika

Cyberbezpieczeństwo to nie tylko zadanie informatyka, bo większość udanych ataków zaczyna się od człowieka, od kliknięcia w link, otwarcia załącznika czy słabego hasła. Skala zagrożeń jest realna. Zespół CERT Polska w 2024 roku otrzymał 600 990 zgłoszeń i zarejestrował 103 449 incydentów bezpieczeństwa, czyli średnio około trzystu dziennie i o 62 procent więcej zgłoszeń niż rok wcześniej[1].

Za bezpieczeństwo danych odpowiada przede wszystkim administrator, czyli urząd — to on, zgodnie z artykułem 32 RODO, musi wdrożyć odpowiednie środki techniczne i organizacyjne. Każdy pracownik ma jednak obowiązek stosować te zasady i przetwarzać dane wyłącznie na polecenie administratora (artykuł 29 RODO). Naruszenia bywają kosztowne. W 2025 roku łączna kwota kar Prezesa UODO przekroczyła 64 miliony złotych[2], a jedna z najgłośniejszych spraw dotyczyła podmiotów publicznych, gdy Poczta Polska otrzymała karę 27 milionów złotych, a Minister Cyfryzacji 100 tysięcy złotych (decyzja UODO z 2025 roku, w 2026 roku nieprawomocnie uchylona przez sąd)[3].

600 990
zgłoszeń

103 449
incydentów

+62%
rok do roku

~300
incydentów/dzień

🏛 **Ostatnie miesiące pokazują, że to nie teoria: w październiku 2025 roku ofiarą ataku ransomware padł Urząd Miejski w Wadowicach, a w 2026 roku podobne incydenty dotknęły kolejne jednostki, w tym gminę Obrazów; po ataku na urząd w Lewinie Kłodzkim wójt apelował do mieszkańców o zastrzeżenie numeru PESEL, bo przestępcy mogli uzyskać dostęp do ich danych[4].**

Silne hasła

Hasło to pierwsza linia obrony. Trzymaj się kilku prostych zasad. Dobre hasło ma co najmniej 12 znaków, a najlepiej 15 lub więcej, i opiera się raczej na czterech albo większej liczbie słów niż na pojedynczym wyrazie. Powinno łączyć litery, cyfry i znaki specjalne, a do każdego systemu należy używać innego hasła. Nigdy nie zapisuj haseł na karteczkach przyklejonych do monitora ani w pliku „hasła.docx", bo to pierwsze miejsce, które sprawdzi intruz. Różnicę widać od razu w zestawieniu poniżej.

Słabe hasło	Mocne hasło
admin123, kowalski1980	Poranna-Kawa-3-Koty!
password, 12345	M0j@Rower-Jesień-Mocne-Hasło9

💡 **Najwygodniejszym rozwiązaniem jest menedżer haseł, na przykład Bitwarden lub KeePass: pamiętasz wtedy tylko jedno hasło główne, a resztę program generuje i bezpiecznie przechowuje. Co jakiś czas sprawdzaj też na stronie haveibeenpwned.com, czy Twój służbowy adres nie pojawił się w znanych wyciekach.**

Uwierzytelnianie dwuskładnikowe (2FA)

Uwierzytelnianie dwuskładnikowe to logowanie za pomocą dwóch elementów – hasła i jednorazowego kodu albo potwierdzenia w aplikacji. Nawet jeśli ktoś pozna Twoje hasło, bez tego drugiego składnika się nie zaloguje. Dlatego 2FA powinno być włączone obowiązkowo dla ePUAP, systemów Elektronicznego Zarządzania Dokumentacją (EZD), systemów finansowo-księgowych, baz z danymi osobowymi oraz wszystkich kont administratorów.

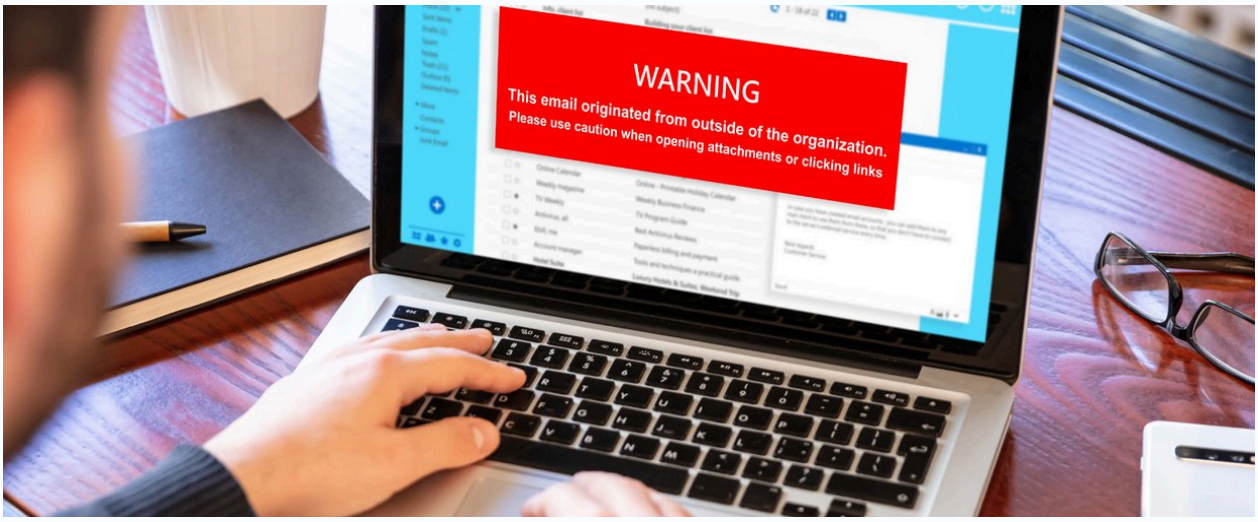
Poszczególne metody różnią się siłą zabezpieczenia. Najsilniejszy jest klucz sprzętowy działający w standardzie FIDO2, dalej aplikacja uwierzytelniająca w rodzaju Google lub Microsoft Authenticator, a dopiero na końcu kod SMS, który lepiej traktować jako rozwiązanie ostateczne. Według amerykańskiej agencji CISA to właśnie odporne na phishing 2FA oparte na standardzie FIDO2 i WebAuthn najlepiej chroni przed phishingiem, atakami push-bombing i przejęciem numeru telefonu. Klucze sprzętowe warto więc wdrażać w pierwszej kolejności dla kont administratorów, poczty i systemów krytycznych; to samo podejście potwierdzają wytyczne ENISA do dyrektywy NIS2[5]. Niezależnie od wybranej metody zachowaj kody odzyskiwania w bezpiecznym miejscu, bo pozwolą odzyskać dostęp w razie utraty telefonu czy klucza.

hasło **drugi składnik (aplikacja lub klucz sprzętowy)** **dostęp**

Phishing

Phishing to próba wyłudzenia danych lub pieniędzy przez podszywanie się pod znaną instytucję, na przykład bank, ZUS, dostawcę energii czy przełożonego. Sprawcy wykorzystujący tę metodę grają na emocjach i presji czasu, posługując się hasłami w rodzaju „pilne", „ostatnie ostrzeżenie" albo „dopłać 1 zł". Sygnałem ostrzegawczym jest nieoczekiwany e-mail lub SMS, adres nadawcy inny niż deklarowana nazwa, link prowadzący gdzie indziej, niż informuje przekaz, błędy językowe oraz prośba o podanie danych lub szybką płatność. ⚠ Sama kłódka przy adresie nie gwarantuje bezpieczeństwa, bo oszuści również korzystają z HTTPS.

Reakcja na podejrzaną wiadomość jest prosta: nie klikaj w link ani nie otwieraj załącznika, zgłoś sprawę do działu IT lub inspektora ochrony danych, a następnie ostrzeż zespół, ponieważ phishing zwykle trafia do wielu osób naraz. Podejrzanego SMS-a możesz bezpłatnie przekazać na numer 8080 prowadzony przez CERT Polska, a wątpliwy e-mail zgłosić na adres cert@cert.pl.



Ransomware

Ransomware to złośliwe oprogramowanie, które szyfruje pliki i żąda okupu, a często także kradnie dane i grozi ich ujawnieniem. Skutek jego działania bywa dla urzędu poważny, bo oznacza paraliż pracy, powrót do obsługi papierowej i ryzyko ujawnienia danych mieszkańców. Gdy zobaczysz żądanie okupu lub zablokowane pliki, najpierw odłącz komputer od sieci, wyciągając kabel albo wyłączając Wi-Fi, żeby atak się nie rozprzestrzeniał. Nie płać okupu i nie próbuj naprawiać sytuacji samodzielnie ani negocjować z przestępcami. Następnie niezwłocznie zgłoś incydent przełożonemu, działowi IT oraz inspektorowi ochrony danych.

Wycieki danych i bezpieczna wymiana plików

Najczęstsze przyczyny wycieków to ataki i złośliwe oprogramowanie, błędna konfiguracja, na przykład pozostawiony otwarty folder w chmurze, zwykły błąd ludzki w rodzaju wysłania pliku do niewłaściwej osoby, a także zguba lub kradzież sprzętu. 🏛 Wystarczy jedna omyłka: zgubiony pendrive z danymi setek osób czy e-mail z listą numerów PESEL wysłany do nieprawidłowego odbiorcy to realne przyczyny kar i strat wizerunkowych w polskich instytucjach[4].

Bezpieczna wymiana plików opiera się na kilku zasadach. Wewnątrz urzędu korzystaj z systemu EZD z kontrolą dostępu oraz z szyfrowanych folderów, a na zewnątrz przesyłaj dokumenty przez ePUAP lub e-Doręczenia, najlepiej z szyfrowanymi załącznikami. ⚠ Do danych osobowych nigdy nie używaj prywatnej poczty, komunikatorów ani przypadkowych pendrive'ów. Pamiętaj też, że urząd może bezpłatnie zarejestrować swoje domeny w serwisie moje.cert.pl prowadzonym przez CERT Polska i NASK, zlecić ich automatyczne skanowanie pod kątem podatności i błędnych konfiguracji oraz otrzymywać alerty o wyciekach haseł i infekcjach, co jest prostym, wdrażalnym od ręki sposobem na bieżącą kontrolę bezpieczeństwa strony i infrastruktury[6].

Reakcja na incydent krok po kroku

Gdy dojdzie do incydentu, liczy się spokój i właściwa kolejność działań:

1. Powiadom natychmiast przełożonego, dział IT i inspektora ochrony danych.

2. Ogranicz szkodę, odłączając urządzenie od sieci i unikając zbędnych działań.

3. Zachowaj dowody, czyli zrzuty ekranu, podejrzane e-maile i logi.

4. Zgłoś incydent do CERT Polska przez formularz incydent.cert.pl, zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa.

5. Przy naruszeniu danych osobowych zgłoś je Prezesowi UODO w ciągu 72 godzin (artykuł 33 RODO).

6. Udokumentuj każdy krok: daty, godziny, osoby i czynności.

Własną procedurę urząd najlepiej oprze na zaktualizowanym poradniku UODO z lutego 2025 roku, który zawiera gotowe wzory zgłoszeń naruszeń, studia przypadków i rekomendacje oceny ryzyka. Na jego podstawie dobrze jest przygotować wewnętrzny rejestr naruszeń i wzór zgłoszenia, aby w razie incydentu działać szybko i zgodnie z artykułem 33 RODO[7].

W skrócie. *Stosuj długie, unikalne hasła w menedżerze i włącz 2FA wszędzie, gdzie pracujesz z danymi, najlepiej w postaci klucza sprzętowego. Nie klikaj w nieoczekiwane linki, weryfikuj „pilne" prośby innym kanałem, a dane wymieniaj wyłącznie przez EZD, ePUAP lub e-Doręczenia, nigdy przez prywatną pocztę. W razie ataku ransomware odłącz sprzęt od sieci i nie płać okupu. Każdy incydent zgłoś działowi IT i inspektorowi ochrony danych oraz do CERT Polska, a przy naruszeniu danych osobowych Prezesowi UODO w ciągu 72 godzin. Pamiętaj o numerze 8080 do zgłaszania phishingowych SMS-ów.*

Rozdział 3. Zarządzanie danymi i otwieranie danych

Ten rozdział pokazuje, jak na co dzień pracować z danymi mieszkańców zgodnie z RODO, kiedy sięgać po anonimizację, a kiedy po pseudonimizację, czym są dane otwarte na portalu dane.gov.pl oraz dlaczego interoperacyjność systemów ułatwia życie urzędnikowi i obywatelowi.

Dane to paliwo nowoczesnego urzędu

Urząd codziennie przetwarza ogromne ilości danych, od wniosków i decyzji po rejestry i korespondencję. Sposób, w jaki nimi zarządzasz, decyduje zarówno o bezpieczeństwie mieszkańców, jak i o jakości usług. Cały ten materiał porządkują trzy obszary: ochrona danych osobowych zgodnie z RODO, otwieranie danych publicznych oraz interoperacyjność systemów.

Skala problemu jest realna. W 2024 roku do UODO wpłynęło 14 842 zgłoszenia naruszeń ochrony danych[1]. Najczęstsza przyczyna nie była spektakularnym atakiem hakerskim, lecz prozaicznym błędnym zaadresowaniem korespondencji, czyli czymś, co zdarza się w każdym urzędzie.

Ochrona danych osobowych w praktyce

RODO opiera się na kilku zasadach, które dobrze mieć stale z tyłu głowy. Minimalizacja oznacza, że zbierasz tylko dane naprawdę potrzebne. Ograniczenie celu nakazuje używać danych wyłącznie do celu, dla którego je zebrano. Integralność i poufność to obowiązek chronienia danych przed dostępem osób nieuprawnionych. Rozliczalność wreszcie wymaga, byś potrafił wykazać, że tych zasad przestrzegasz. Jednym z praktycznych standardów ich stosowania są wytyczne Europejskiej Rady Ochrony Danych 01/2025, w których traktuje się pseudonimizację jako uznany środek bezpieczeństwa w rozumieniu artykułu 32 RODO, a nie jako zwolnienie z obowiązków[2].

Anonimizacja czy pseudonimizacja?

To dwa różne narzędzia, których nie należy mylić. Anonimizacja polega na nieodwracalnym usunięciu danych identyfikujących, dzięki czemu dane przestają być danymi osobowymi i nie podlegają już RODO. Pseudonimizacja natomiast zastępuje identyfikatory kodami, na przykład zamienia „Jana Kowalskiego" na „ID-4821", przy czym proces ten można cofnąć za pomocą osobno przechowywanego klucza. Najważniejsza konsekwencja jest taka, że dane spseudonimizowane wciąż pozostają danymi osobowymi chronionymi przez RODO. W poniższej tabeli zestawiono obie ścieżki.

	Anonimizacja	Pseudonimizacja
Na czym polega	nieodwracalne usunięcie danych identyfikujących	zastąpienie identyfikatorów kodami (np. „Jan Kowalski" → „ID-4821")
Czy można cofnąć	nie	tak, przy użyciu osobno przechowywanego klucza
Status prawny	dane przestają być danymi osobowymi	dane nadal są danymi osobowymi (chronione RODO)

⚠️ **Sama pseudonimizacja nie zwalnia z obowiązków RODO, bo to wciąż dane osobowe.**

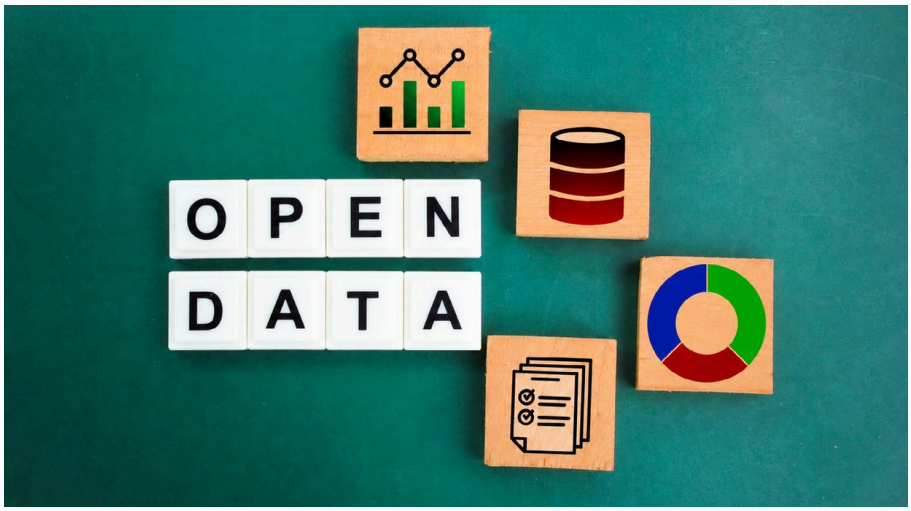
Kary Prezesa UODO dotykają także podmioty publiczne. Jedną z pierwszych nałożono na burmistrza (40 tysięcy złotych), kolejne między innymi na Głównego Geodetę Kraju (100 tysięcy złotych) oraz na sąd rejonowy. Najczęściej wiążą się one z zarzutem braku odpowiednich zabezpieczeń lub umów powierzenia danych[3]. Stąd prosta zasada na co dzień: nie udostępniaj danych osobowych „na wszelki wypadek" i nie publikuj plików z ukrytymi danymi, takimi jak numer PESEL schowany w niewidocznej kolumnie arkusza.

Dane otwarte

Dane otwarte to informacje publiczne udostępniane bezpłatnie, w formacie maszynowym, takim jak CSV czy JSON, na licencji pozwalającej na dowolne ponowne wykorzystanie. Dobre dane otwarte spełniają trzy warunki naraz: opierają się na otwartej licencji, którą można swobodnie wykorzystać, także komercyjnie, umożliwiają ponowne wykorzystanie bez sztucznych barier i wraz z metadanymi, a także mają otwarty format, czyli na przykład plik CSV zamiast skanu. Różnica bywa subtelna, ale istotna, bo PDF nadaje się do czytania, lecz słabo do automatycznego przetwarzania, podczas gdy ten sam zbiór zapisany w CSV staje się naprawdę otwarty.

Centralnym miejscem jest portal dane.gov.pl, na którym zamieszczane są dziesiątki tysięcy zbiorów wraz z metadanymi i dostępem przez API[4]. Na otwartych danych powstają praktyczne aplikacje obywatelskie, od rozkładów jazdy po mapy usług i statystyki. Publikując dane, traktuj zbiory o wysokiej wartości, czyli HVD, takie jak dane geoprzestrzenne, środowiskowe, meteorologiczne, statystyczne, o spółkach czy mobilności, jako obowiązkowo udostępniane bezpłatnie, w formacie nadającym się do odczytu maszynowego i przez API; obowiązek ten wynika z rozporządzenia wykonawczego (UE) 2023/138 i obowiązuje od 9 czerwca 2024 roku[5]. Zanim zlecisz zbieranie danych „od zera", sprawdź, czy potrzebny zbiór nie jest już dostępny na dane.gov.pl, a publikowane zbiory zawsze opisuj metadanymi mówiącymi, co zawierają, kiedy powstały i w jakim formacie, bo to one realnie ułatwiają ponowne użycie.

Dobrze pokazują to dwa przykłady udanego otwierania danych. Centralna Ewidencja Emisyjności Budynków prowadzona przez GUNB dowodzi, że dane publiczne można udostępniać bez ujawniania danych prywatnych, udostępniając je w sposób ograniczający identyfikację pojedynczych osób, między innymi przez agregację i kontrolę dostępu[6]. Ubezpieczeniowy Fundusz Gwarancyjny, otwierając dane o polisach OC, pozwolił z kolei każdemu bezpłatnie sprawdzić ubezpieczenie pojazdu online[7].



Interoperacyjność

Interoperacyjność to zdolność różnych systemów i urzędów do wymiany danych oraz współdziałania bez ręcznego przepisywania. Gdy gmina, ZUS i bank „rozmawiają" wspólnym językiem opartym na standardach, takich jak XML, JSON czy REST API, sprawa mieszkańca toczy się szybciej i z mniejszą liczbą błędów. Podstawą są Krajowe Ramy Interoperacyjności (KRI), czyli wspólne standardy techniczne i zasady wymiany informacji elektronicznej. Na tej samej podstawie prawnej (ustawa o informatyzacji z 2005 r.) działają między innymi ePUAP oraz Profil Zaufany, z którego korzysta już ponad 13 milionów Polaków i który stanowi klucz do setek e-usług administracji[8].

Zanim poprosisz mieszkańca o zaświadczenie, sprawdź, czy informacja jest już dostępna w rejestrze, do którego urząd ma dostęp. To zasada „pytaj raz" (ang. once-only): nie żądaj od obywatela danych, które państwo już posiada.

Przy incydentach i naruszeniach opieraj się na aktualnych wytycznych Prezesa UODO dotyczących naruszeń ochrony danych (zaktualizowanych w 2025 roku), które porządkują procedurę zgłaszania naruszeń i ocenę ryzyka, tak by na zdarzenia w rodzaju błędnego zaadresowania korespondencji reagować w ciągu 72 godzin[9].

W skrócie. *Zbieraj tylko dane niezbędne i używaj ich wyłącznie do celu, dla którego je zebrano, a przed udostępnieniem upewnij się, że nie ujawniasz danych osobowych, na przykład przez agregację lub pseudonimizację. Pamiętaj, że dane spseudonimizowane to wciąż dane osobowe chronione RODO. Publikując informacje publiczne, zamiast skanu wybieraj otwarty format, czyli CSV lub JSON, i opisuj zbiory metadanymi na dane.gov.pl. Wreszcie korzystaj z rejestrów i zasady „pytaj raz", zamiast żądać od mieszkańca zaświadczeń, które państwo już posiada.*

Rozdział 4. Odporność i higiena cyfrowa urzędnika

Ten rozdział pokazuje, jak dbać o higienę i odporność cyfrową w pracy urzędu: rozpoznawać dezinformację i deepfake, weryfikować informacje, radzić sobie z przeciążeniem oraz chronić ciało przy pracy z komputerem.

Higiena i odporność cyfrowa – dwie strony tej samej monety

Higiena cyfrowa to zestaw codziennych nawyków, dzięki którym bezpiecznie i zdrowo korzystasz z technologii. Składają się na nią porządek w plikach, przerwy od ekranu i świadome zarządzanie powiadomieniami. Odporność cyfrowa idzie o krok dalej i oznacza zdolność radzenia sobie z wyzwaniami świata cyfrowego. Opiera się na trzech filarach. Pierwszym jest dobrostan, czyli umiejętność niepoddawania się nadmiarowi bodźców, powiadomień i hejtu. Drugim jest bezpieczeństwo, czyli odporność na oszustwo i manipulację. Trzecim jest powrót do równowagi, czyli zdolność wrócenia do normalnej pracy po kryzysie, takim jak atak, awaria czy fala krytyki. Higiena i odporność to dwie strony tej samej monety: dobre nawyki budują codzienną stabilność, a odporność pozwala przetrwać sytuacje wyjątkowe.

Dezinformacja, fake news i deepfake

Dezinformacja to celowe rozpowszechnianie fałszywych informacji po to, by wprowadzić odbiorcę w błąd. Dziś jest to zagrożenie pierwszej wagi. W raporcie Global Risks Report 2025 Światowego Forum Ekonomicznego dezinformację wskazano jako najpoważniejsze zagrożenie krótkoterminowe, i to drugi rok z rzędu[1].

W Polsce skala problemu rośnie. Organizacja fact-checkingowa Demagog podsumowała, że w 2025 roku aż 65 procent zweryfikowanych wypowiedzi polityków okazało się fałszem lub manipulacją, co oznacza wzrost o 17 punktów procentowych w stosunku do poprzedniego roku[2]. W razie wątpliwości sprawdź fakty w serwisach fact-checkingowych, takich jak Demagog, zanim podasz informację dalej.

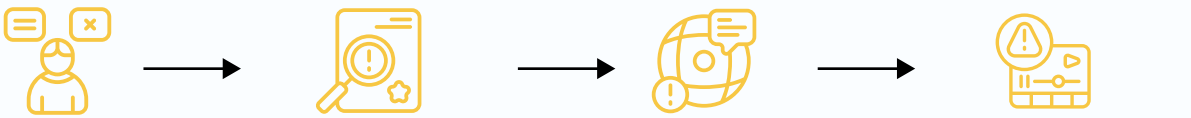
Osobnym, coraz groźniejszym zjawiskiem jest deepfake, czyli spreparowane nagranie audio lub wideo, w którym sztuczna inteligencja podmienia twarz albo głos. Takie materiały są coraz trudniejsze do odróżnienia

od prawdy. Zespół CSIRT KNF wielokrotnie ostrzegał przed „fałszywymi inwestycjami", w których oszuści wykorzystują deepfake i wizerunki znanych osób oraz podszywają się pod instytucje finansowe i spółki Skarbu Państwa, by wyłudzić dane i pieniądze[3]. To realne ryzyko także dla urzędnika, który publikuje i odbiera informacje w imieniu instytucji. Problem pogłębia fakt, że według badań blisko 40 procent Polaków w ogóle nie weryfikuje informacji znalezionych w sieci, a urzędnik jako źródło informacji publicznej ponosi tu szczególną odpowiedzialność.

Reakcją instytucji na ten rosnący problem są gotowe narzędzia, z których urząd może korzystać. Ministerstwo Cyfryzacji i NASK prowadzą kampanię „Nie bądź internetowym trollem", której darmowe materiały edukacyjne nadają się do szkolenia pracowników z rozpoznawania dezinformacji, a podejrzane treści można zgłaszać przez oficjalny formularz na nask.pl/dezinfo[6]. Warto wykorzystać ten gotowy, instytucjonalny kanał reagowania zamiast samodzielnie prostować treści w sieci. Coraz większą rolę będzie też odgrywać prawo: artykuł 50 unijnego AI Act, który zacznie obowiązywać 2 sierpnia 2026 roku, nakłada obowiązek wyraźnego oznaczania deepfake'ów oraz treści wytworzonych lub zmodyfikowanych przez sztuczną inteligencję, a Komisja Europejska udostępnia do tego zestaw ikon[7]. Urząd publikujący materiały z udziałem AI powinien je etykietować, a odbierając cudze treści, traktować brak takiego oznaczenia jako sygnał ostrzegawczy.

Jak weryfikować informacje

Weryfikacja informacji opiera się na czterech prostych odruchach, które wykonuj zawsze przed udostępnieniem treści. Najpierw sprawdź źródło i zapytaj, kto opublikował dany materiał oraz czy jest to wiarygodna, możliwa do zidentyfikowania instytucja. Następnie porównaj informację z innymi źródłami i sprawdź, czy potwierdzają ją niezależne, rzetelne media i instytucje. Trzeci krok to sprawdzenie daty i kontekstu, czyli upewnienie się, że informacja jest aktualna i nie została wyrwana z kontekstu. Na koniec zweryfikuj obrazy i nagrania, szukając oznak manipulacji oraz korzystając z wyszukiwania obrazem i narzędzi wykrywających treści generowane przez AI. Odporność jest przy tym zespołowa: ucz cały zespół rozpoznawania phishingu oraz dezinformacji i nie udostępniaj dalej treści, której nie zweryfikowałeś.



Dobrym ćwiczeniem jest darmowa gra „Bad News" (getbadnews.com/pl), w której wcielasz się w twórcę fałszywych newsów i poznajesz techniki manipulacji od kuchni, dzięki czemu łatwiej je później rozpoznać w realnym świecie[8].

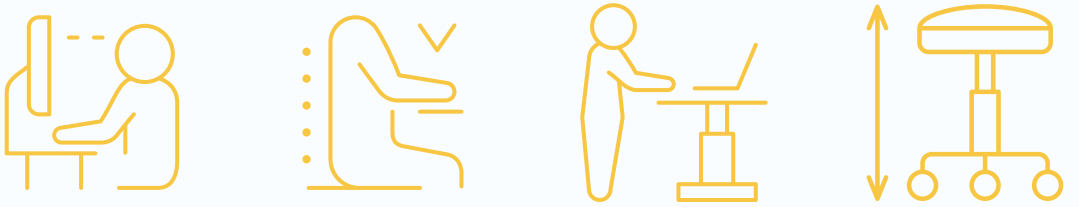
Przeciążenie informacyjne

Przeciążenie informacyjne to stan, w którym ilość i tempo napływających informacji przekraczają nasze możliwości ich przetworzenia. W urzędzie oznacza to natłok e-maili, przepisów, zapytań i powiadomień. Tempo pracy realnie przyspiesza. Według badań Microsoft Work Trend Index aktywność pracowników bywa przerywana średnio co kilka minut przez powiadomienie, mail lub czat[4]. Skutkiem są gorsza koncentracja, częstsze błędy, stres i wypalenie.

Radzenie sobie z tym natłokiem zaczyna się od wyznaczenia priorytetów. Badania pokazują, że osoby, które priorytetyzują zadania, tracą mniej czasu na samo zarządzanie pracą. Prowadź więc listę zadań uporządkowaną według ważności. Pomaga też ograniczenie powiadomień: wyłącz te nieistotne i ustal stałe „okna" na sprawdzanie poczty. Wspiera to cyfrowy minimalizm, czyli jedno zadanie naraz i mniej otwartych kart, a także regularne przerwy od ekranu. Dobrze sprawdza się zasada 20-20-20, zgodnie z którą co 20 minut warto spojrzeć przez 20 sekund na obiekt oddalony o około sześć metrów (20 stóp). CIOP-PIB zaleca krótkie, częste przerwy po krótkich okresach pracy zamiast rzadkich i długich, co urzędnik może wdrożyć od razu, planując mikroprzerwy w kalendarzu[9]. ⚠ Praca „na okrągło" w trybie ciągłych powiadomień to prosta droga do błędów.

Ergonomia – zadbaj o ciało, nie tylko o dane

Praca przy komputerze obciąża nie tylko uwagę, ale i ciało, a większość pracowników biurowych doświadcza bólu kręgosłupa. Podstawą profilaktyki jest prawidłowa pozycja przy biurku. Kolana i łokcie powinny być zgięte pod kątem zbliżonym do 90 stopni, plecy proste i oparte o oparcie krzesła, a stopy płasko ułożone na podłodze lub na podnóżku. Ekran najlepiej ustawić w odległości od 40 do 75 centymetrów od oczu, z górną krawędzią na wysokości wzroku. Pomocnym uzupełnieniem jest poradnik CIOP „Ćwiczenia fizyczne w miejscu pracy", w którym znajdziesz proste ćwiczenia przy biurku przeciw sztywności i bólowi[5].



40 – 75 cm od ekranu | **90° w łokciach i kolanach** | **ekran na wysokości wzroku** | **stopy na podłodze**

W skrócie. *Zanim udostępnisz informację, sprawdź źródło, datę i kontekst, a podejrzane zdjęcia lub nagrania traktuj jak możliwy deepfake i nie ufaj „pilnym, niepowtarzalnym ofertom" z wizerunkami znanych osób. Korzystaj z gotowych narzędzi instytucji, takich jak fact-checking Demagoga i formularz NASK, zamiast prostować treści samodzielnie. Panuj nad natłokiem informacji, prowadząc listę zadań priorytetowych, wyłączając zbędne powiadomienia i ustalając „okna" na sprawdzanie poczty. Rób krótkie, częste przerwy od ekranu według zasady 20-20-20 i zadbaj o ergonomię stanowiska, bo odporność cyfrowa to także zdrowe ciało.*

Rozdział 5. Aplikacje krajowe i e-administracja

Ten rozdział pokazuje, jak rozpoznawać kluczowe krajowe narzędzia e-administracji, korzystać z tożsamości cyfrowej i prowadzić urzędową korespondencję elektroniczną, a także jak doradzić mieszkańcowi i przedsiębiorcy, gdzie załatwią sprawę online.

Dlaczego znajomość aplikacji krajowych się opłaca

Cyfrowe narzędzia administracji skracają czas obsługi, obniżają koszty i poprawiają jakość usług. Dla urzędnika to konkretne ułatwienie: mniej papieru, szybszy obieg spraw i bezpieczniejsza komunikacja. Wspólnym kluczem do większości e-usług pozostaje Profil Zaufany, z którego korzysta już ponad 13 milionów Polaków[1]. Znajomość cyfrowych narzędzi pozwala nie tylko sprawniej wykonywać własną pracę, ale też trafnie kierować mieszkańców tam, gdzie sprawę da się załatwić bez wizyty w urzędzie.

Tożsamość cyfrowa

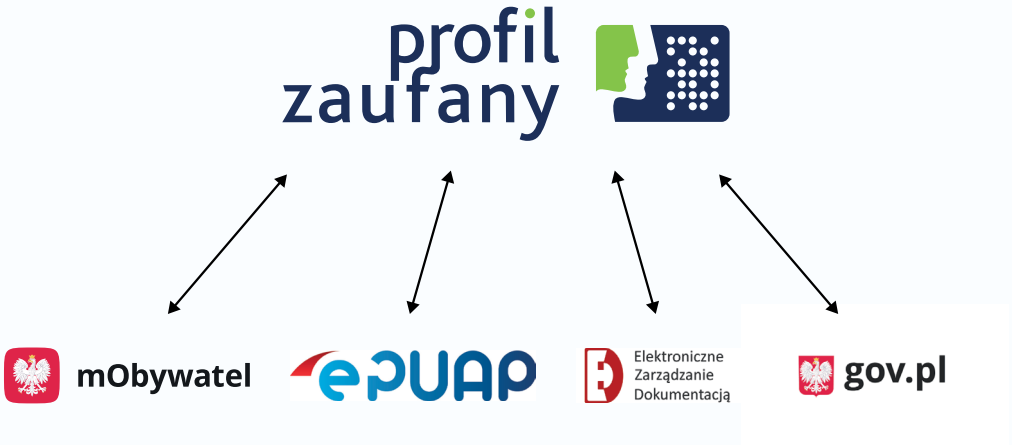
Profil Zaufany to bezpłatne narzędzie do potwierdzania tożsamości w sieci i składania podpisu zaufanego, prawnie skutecznego w kontaktach z administracją. Umożliwia on logowanie do setek usług publicznych jednym kontem, co czyni go fundamentem całego ekosystemu e-administracji.

mObywatel to bezpłatna aplikacja na telefon, dziś według Ministerstwa Cyfryzacji, najpopularniejsza aplikacja rządowa w Europie[2]. Zawiera między innymi mDowód, czyli elektroniczny dokument tożsamości prawnie zrównany z plastikowym dowodem osobistym na terenie Polski (nie służy jednak jako dokument podróży za granicę); wydano już ponad 12 milionów mDowodów (stan: maj 2026)[2]. W aplikacji znajdziesz również dokumenty, powiadomienia i e-usługi, które honoruj na co dzień i polecaj mieszkańcom. mDowód można przyjmować jako pełnoprawny dokument tożsamości przy obsłudze i legitymowaniu, a aplikacja udostępnia praktyczne funkcje, takie jak okazywanie e-recepty kodem QR bez podawania numeru PESEL na głos, usługa Zastrzeż PESEL czy pobieranie zaświadczenia z Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG)[6].

🏛 Co to znaczy dla urzędu: mieszkaniec może potwierdzić tożsamość mDowodem, na przykład przy odbiorze sprawy, a dokument podpisać podpisem zaufanym, wszystko bez wizyty i bez papieru. Spójrz też w przyszłość. Zgodnie z rozporządzeniem (UE) 2024/1183 (eIDAS 2.0) każde państwo członkowskie musi udostępnić obywatelom Europejski Portfel Tożsamości Cyfrowej (EUDI Wallet) do końca 2026 roku, a obowiązek jego akceptowania przez podmioty zobowiązane wejdzie w życie do końca 2027 roku[7]. Już teraz warto planować procedury obsługi mieszkańców posługujących się portfelem, także tych z innych krajów Unii.

Urzędowa korespondencja elektroniczna

ePUAP to platforma usług administracji: katalog usług, składanie wniosków i odbiór urzędowych poświadczeń (UPP/UPO). e-Doręczenia są natomiast elektronicznym odpowiednikiem listu poleconego za potwierdzeniem odbioru i stają się domyślnym kanałem urzędowej korespondencji. Obowiązek jest wprowadzany etapami: od 1 stycznia 2025 roku obejmuje podmioty publiczne oraz osoby wykonujące zawody zaufania publicznego, a od 1 kwietnia 2025 roku firmy zarejestrowane w KRS przed 1 stycznia 2025 roku[3] [8].



⚠ Ważne dla urzędnika: jeśli mieszkaniec lub firma ma adres do e-Doręczeń, to właśnie tam, a nie poprzez list papierowy, kierujesz korespondencję. Zanim wyślesz pismo listem poleconym, sprawdź w Bazie Adresów Elektronicznych, czy adresat ma adres do e-Doręczeń. Gdy taki adres istnieje, korespondencja elektroniczna jest tańsza i szybsza.

Obieg dokumentów, chmura i dane

Elektroniczne Zarządzanie Dokumentacją to system prowadzenia spraw i akt w postaci elektronicznej, z dekretacją, kontrolą dostępu i archiwizacją. Coraz częściej zastępuje papierowy obieg w urzędach, eliminując drukowanie dokumentów wyłącznie po to, by je podpisać. Chmura krajowa to rozwiązania chmurowe dla sektora publicznego, obejmujące usługi IaaS, PaaS i SaaS; dla administracji rządowej rozwijana jest Rządowa Chmura Obliczeniowa (RChO), chmura.gov.pl. Pozwalają one optymalizować koszty i bezpieczeństwo bez utrzymywania własnej serwerowni. Dane publiczne udostępniane są natomiast na stronie dane.gov.pl (zob. Rozdział 3) i są one elementem tego samego, spójnego ekosystemu.

Usługi dla przedsiębiorców (które urzędnik powinien znać)

Centralna Ewidencja i Informacja o Działalności Gospodarczej służy do rejestracji, zmiany i zawieszenia firmy oraz jest publicznym, wiarygodnym źródłem danych o przedsiębiorcach, dostępnym w serwisie biznes.gov.pl. Krajowy System e-Faktur (KSeF) to obowiązkowa od 2026 roku platforma e-faktur ustrukturyzowanych; obowiązek jest wprowadzany etapami – od 1 lutego 2026 roku dla największych podatników i od 1 kwietnia 2026 roku dla pozostałych[4], co zmienia obieg dokumentów księgowych także w jednostkach publicznych.

Dobra praktyka: zanim poprosisz przedsiębiorcę o dane firmy, sprawdź je w CEIDG lub KRS. To często szybsze i pewniejsze niż zaświadczenie i pozwala – zgodnie z zasadą „pytaj raz" (zob. Rozdział 3) – nie żądać danych, które są już w publicznych rejestrach.

Bezpieczeństwo i interoperacyjność

Wszystkie te systemy łączą wspólne standardy wymiany danych (interoperacyjność, KRI, zob. Rozdział 3) oraz wymogi bezpieczeństwa (ochrona danych osobowych zgodnie z RODO, uwierzytelnianie dwuskładnikowe – 2FA i kontrola dostępu, zob. Rozdział 2). Dzięki temu „rozmawiają" ze sobą i chronią dane mieszkańców, tworząc całość, w której tożsamość cyfrowa, korespondencja i rejestry współpracują w sposób bezpieczny i przewidywalny.

W skrócie. *Profil Zaufany i mObywatel z mDowodem to fundament tożsamości cyfrowej, który urząd powinien honorować na co dzień; mDowód jest tak samo ważny jak dowód plastikowy. Korespondencję kieruj przez e-Doręczenia zawsze, gdy adresat ma adres w Bazie Adresów Elektronicznych, zamiast wysyłać list papierowy. Korzystaj z EZD i podpisu zaufanego zamiast drukowania „dla podpisu", a dane przedsiębiorców weryfikuj w CEIDG i KRS, nie żądając zbędnych zaświadczeń. Pamiętaj o KSeF i Europejskim Portfelu Tożsamości Cyfrowej, który urzędy będą musiały zacząć akceptować do końca 2026 roku.*

Rozdział 6. Komunikacja w pracy zdalnej

Ten rozdział pokazuje, jak bezpiecznie poprowadzić spotkanie online, sprawnie korzystać z kalendarzy i chmury oraz zachować zgodność z RODO, kiedy pracujesz poza biurem.

Praca zdalna i hybrydowa w urzędzie

Praca zdalna i hybrydowa to dziś stały element administracji. Daje elastyczność i oszczędność czasu przeznaczanego wcześniej na dojazdy, ale stawia też wyzwania: utrudnia komunikację, ochronę danych i samodyscyplinę[1]. Klucz tkwi w dobrych narzędziach i jasnych zasadach, a o nich właśnie jest ten rozdział. Najwięcej zyskują zespoły, które z góry ustalają godziny dostępności, akceptowalny czas odpowiedzi i kanały do poszczególnych spraw, bo wtedy elastyczność nie zamienia się w chaos.

Spotkania online

Najczęściej używane platformy w administracji to Microsoft Teams, Zoom i Google Meet. Niezależnie od wyboru dobre spotkanie zaczyna się od przygotowania. Wyślij zaproszenie z agendą, w której każdy punkt ma swoją godzinę, podlinkuj potrzebne dokumenty, na przykład prezentację czy plik tekstowy, tak aby wszystko było w jednym miejscu, oraz dopisz oczekiwania wobec uczestników, choćby prośbę o przygotowanie jednego lub dwóch przykładów z własnej pracy.

5 reguł bezpiecznego spotkania online

brak danych wrażliwych w zaproszeniu

link tylko do uprawnionych

hasło lub poczekalnia

zgoda na nagrywanie

brak udostępniania nagrań osobom postronnym

Spotkanie online to także przetwarzanie danych, więc obowiązują tu zasady RODO. W treści zaproszenia nie umieszczaj danych wrażliwych, link wysyłaj wyłącznie do osób uprawnionych i nigdy nie publikuj go otwarcie, a przed wpuszczeniem uczestników włącz hasło lub poczekalnię. O nagrywaniu musisz poinformować uczestników i uzyskać ich zgodę, a samych nagrań ani notatek nie udostępniaj osobom, które w spotkaniu nie brały udziału. W praktyce najlepiej z góry włączyć ustawienia, które domykają te reguły: silne hasło, poczekalnię, blokadę udostępniania ekranu i czatu prywatnego przez uczestników, wyłączone automatyczne nagrywanie oraz wyłączony transfer plików.

Te zalecenia mają mocne oparcie w wytycznych instytucji bezpieczeństwa. Brytyjskie NCSC radzi, by na koncie administratora włączyć dwuetapową weryfikację lub klucze dostępu, dopuszczać tylko uwierzytelnionych i zaproszonych uczestników, a od pozostałych wymagać kodu dostępu i weryfikować ich w poczekalni; przypomina też, by sprawdzać, gdzie trafiają nagrania, transkrypcje i pliki oraz kto ma do nich dostęp[4].

Polski UODO dorzuca praktyczną wskazówkę o minimalizacji danych: podczas wideokonferencji lepiej posługiwać się służbowym adresem e-mail lub pseudonimem niż pełnymi danymi. Warto też przeskanować program antywirusem i zapoznać się z polityką prywatności usługi. Obrazu i głosu uczestników nie wolno nagrywać bez podstawy i ich wiedzy[5].

Kalendarze i organizacja pracy

Synchronizuj pracę przez kalendarz, na przykład Microsoft Outlook lub Google Calendar: planuj w nim spotkania, ustawiaj przypomnienia i informuj zespół o swojej dostępności. Kalendarze współdzielone, obejmujące dyżury, spotkania i urlopy, porządkują pracę zespołu i ułatwiają obsługę mieszkańców, o czym więcej w Rozdziale 8. Najlepiej ustalić jeden wspólny kalendarz dyżurów i jeden sposób oznaczania nieobecności, bo wtedy znika powracające pytanie: „Kto dziś jest?”.

Współdzielenie i wymiana plików

Zamiast wysyłać mailem kolejne wersje tego samego pliku, pracujcie wspólnie w chmurze, korzystając z OneDrive czy Google Drive. Zyskujecie dzięki temu dostęp z każdego urządzenia, automatyczne kopie zapasowe, możliwość pracy wielu osób na jednym dokumencie oraz historię zmian, która zastępuje mnożenie plików typu „final_2_ostateczny”. Dostęp trzeba jednak świadomie kontrolować: udostępniaj konkretnym osobom, a nie „każdemu, kto ma link”, przypisuj role odpowiednie do potrzeb, czyli odczyt, komentowanie lub edycję, a odbiorcom zewnętrznym nadawaj dostęp tylko na czas, który jest naprawdę potrzebny. Danych osobowych mieszkańców nie wrzucaj do prywatnych chmur ani komunikatorów; używaj wyłącznie rozwiązań służbowych z kontrolą dostępu (zob. Rozdział 2).

RODO i bezpieczeństwo w pracy zdalnej

Praca zdalna nie zwalnia z obowiązków ochrony danych. Z dostawcą usługi chmurowej trzeba zawrzeć umowę powierzenia przetwarzania zgodnie z artykułem 28 RODO, przestrzegać zasad przetwarzania i rozliczalności z artykułu 5, a także stosować środki techniczne wymagane przez artykuł 32, takie jak szyfrowanie, kopie zapasowe, testy zabezpieczeń i dwuskładnikowe uwierzytelnianie. Do bezpiecznego, urzędowego obiegu dokumentów służy w Polsce EZD RP, system kancelaryjno-archiwalny stworzony przez NASK, zintegrowany z ePUAP i e-Doręczeniami, swego rodzaju „cyfrowa kancelaria" dla całej administracji[2]. Skala jego wykorzystania rośnie, a wdrożenia, także w modelu chmurowym SaaS dla mniejszych jednostek samorządowych, są finansowane ze środków KPO[2].

W skrócie. *Każde spotkanie online zaczynaj od agendy i podlinkowanych dokumentów, a domyślnie włączaj poczekalnię lub hasło, dopuszczaj tylko zaproszone osoby i pytaj je o zgodę przed nagrywaniem. Pliki trzymaj w chmurze służbowej z kontrolą dostępu i rolami, korzystaj z historii wersji i nigdy nie udostępniaj danych osobowych prywatnymi kanałami. Pamiętaj o umowie powierzenia z dostawcą chmury, włączonym 2FA i aktualnym oprogramowaniu. Do urzędowego obiegu dokumentów używaj krajowego EZD RP, zintegrowanego z ePUAP i e-Doręczeniami.*

Rozdział 7. AI w pracy urzędnika – od teorii do praktyki

Ten rozdział wyjaśnia, czym jest, a czym nie jest sztuczna inteligencja, pokazuje, jak wykorzystać ją do konkretnych zadań urzędowych, w tym z polskimi narzędziami, oraz jak korzystać z niej odpowiedzialnie, rozpoznając ryzyka i działając zgodnie z AI Act i RODO.

Czym jest sztuczna inteligencja

Sztuczna inteligencja (AI) to systemy, które na podstawie ogromnych zbiorów danych uczą się rozpoznawać wzorce i generować odpowiedzi. Przełomem stało się udostępnienie 30 listopada 2022 roku ChatGPT, który pierwszy milion użytkowników zdobył w zaledwie pięć dni[1]. Od tej chwili narzędzia generatywne weszły do codziennej pracy biurowej szybciej niż jakakolwiek wcześniejsza technologia.

Od początku zrozum, jak takie narzędzie działa. ⚠️ Duży model językowy (LLM), taki jak ChatGPT, to system statystyczny przewidujący kolejne słowa, a nie baza wiedzy czy wyrocznia prawna. Potrafi napisać tekst, który brzmi wiarygodnie, ale bywa niezgodny z prawdą, i właśnie z tej cechy wynikają wszystkie dalsze zasady ostrożnego korzystania z AI.

Gdzie AI pomaga urzędnikowi

AI dobrze radzi sobie z zadaniami, które są pracochłonne, ale mają jasny cel. Sprawdza się przy tworzeniu szkicu pisma urzędowego lub ogłoszenia o naborze, przy streszczaniu długiego dokumentu czy ustawy, przy porządkowaniu rozproszonych danych w przejrzystą tabelę oraz przy propozycjach uproszczenia tekstu w duchu prostego języka, o którym mowa w Rozdziale 1. W każdym z tych zastosowań rolą urzędnika pozostaje korekta i odpowiedzialność za efekt końcowy, a AI jedynie przyspiesza pierwszy etap pracy.

Poznaj też rozwiązania tworzone w Polsce, ponieważ lepiej rozumieją nasz kontekst prawny i językowy. PLLuM (Polish Large Language Model) to rządowy, otwarty model językowy rozwijany przez polskich naukowców we współpracy z Ministerstwem Cyfryzacji, dostępny dla wszystkich[2]. Bielik to otwarty polski model stworzony przez Fundację SpeakLeash przy wsparciu superkomputerów Cyfronetu AGH[3]. 💡 Modele otwarte i krajowe można uruchamiać w kontrolowanym środowisku, co sprzyja bezpieczeństwu danych i zgodności z RODO. Do zadań wrażliwych lepiej sięgnąć właśnie po nie.

Ryzyka, o których musisz wiedzieć

Korzystając z AI, trzeba mieć świadomość kilku poważnych ograniczeń. Najgroźniejsze są halucynacje, czyli sytuacje, w których model pewnym tonem podaje nieistniejące przepisy, wyroki czy dane. Do tego dochodzi stronniczość, bo model uczy się na danych, które bywają obciążone uprzedzeniami, oraz ryzyko związane z deepfake'ami i dezinformacją, opisane szerzej w Rozdziale 4. Osobnym zagrożeniem jest wyciek danych: wpisując informacje do otwartego narzędzia, można je w praktyce przekazać dostawcy usługi.

🏛 **Dobrze ilustruje to głośna amerykańska sprawa sądowa, w której prawnik wykorzystał ChatGPT do przygotowania pisma, a model zmyślił nieistniejące wyroki; trafiły one do sądu, a całość skończyła się grzywną nałożoną przez sąd[4]. Wniosek dla urzędnika jest prosty: każdą odpowiedź AI należy traktować jak wstępny projekt do weryfikacji, nigdy jak gotową decyzję.**

Jak dobrze „rozmawiać" z AI, czyli cztery zasady promptu

Jakość odpowiedzi AI zależy wprost od jakości polecenia. Pierwsza zasada to nadanie roli, na przykład poleceniem „Jesteś doświadczonym radcą prawnym do spraw prawa administracyjnego". Druga to jasność i szczegółowość, czyli podanie kontekstu i celu zamiast ogólników. Trzecia to określenie oczekiwanego formatu, na przykład tabeli, szkicu pisma czy listy punktów. Czwarta, najważniejsza, to ochrona danych: nigdy nie wolno wpisywać prawdziwych danych osobowych mieszkańców ani informacji niejawnych do otwartych narzędzi.

Różnicę między poleceniem słabym a dobrym dobrze widać na konkretnych przykładach.

Słaby prompt	Dobry prompt
„Napisz coś o urzędzie gminy".	„Jako specjalista ds. administracji wyjaśnij w pięciu punktach podstawowe obowiązki urzędu gminy wobec mieszkańców".
„Napisz ogłoszenie o pracy".	„Przygotuj projekt ogłoszenia o naborze na stanowisko urzędnicze, uwzględniając wymagania formalne i zakres obowiązków".
Pismo z danymi: „Jan Kowalski ul. Testowa 7…"	„Napisz szkic pisma, używając ogólnych sformułowań, bez konkretnych danych osobowych".

Jak dobrze rozmawiać z AI, czyli cztery zasady promptu.

nadaj role | **pisz jasno i szczegółowo** | **określ format** | **chroń dane**

Prawo: AI Act i odpowiedzialność

Korzystanie z AI w administracji regulują AI Act, czyli rozporządzenie UE 2024/1689, oraz RODO. AI Act wchodzi w życie etapami: zaczął obowiązywać 1 sierpnia 2024 roku, od 2 lutego 2025 roku zakazuje praktyk o niedopuszczalnym ryzyku, od 2 sierpnia 2025 roku wprowadza zasady dla modeli ogólnego przeznaczenia (GPAI), od 2 sierpnia 2026 roku stawia wymogi systemom wysokiego ryzyka, a pozostałe przepisy zaczną obowiązywać od 2 sierpnia 2027 roku[5]. Dla urzędów ważny jest artykuł 4 AI Act, zgodnie z którym od 2 lutego 2025 roku instytucje wdrażające AI mają zapewnić personelowi odpowiedni poziom kompetencji (AI literacy). Pomocne bywa tu bezpłatne unijne repozytorium dobrych praktyk prowadzone przez Komisję Europejską[6].

Z przepisów wynikają cztery praktyczne obowiązki urzędnika. Treści generowane przez AI należy oznaczać w oficjalnych kanałach. Odpowiedzialność za pismo lub decyzję zawsze ponosi człowiek, a nie program. Każda decyzja o skutkach prawnych wymaga więc weryfikacji przez pracownika merytorycznego. Wreszcie obowiązuje ochrona danych, czyli zakaz wprowadzania danych osobowych i informacji niejawnych do otwartych, niezabezpieczonych narzędzi AI.

Własnych zasad korzystania z generatywnej AI urząd nie musi pisać od zera. Może oprzeć je na rządowym Przewodniku dla administracji publicznej Ministerstwa Cyfryzacji, który zawiera praktyczne wskazówki dotyczące projektów pism, streszczeń i porządkowania informacji, omówienie wymogów AI Act i RODO oraz checklistę decyzyjną pomagającą ocenić, czy i jak bezpiecznie wdrożyć dane narzędzie w konkretnej sprawie[7]. Inspiracji warto też szukać za granicą: w brytyjskim rządowym AI Playbooku zamieszczono gotowy zestaw 10 zasad odpowiedzialnego użycia AI oraz checklisty na końcu każdej sekcji, w tym obowiązek rozumienia ograniczeń AI i utrzymania nadzoru człowieka nad każdą istotną decyzją – można go potraktować jako wzorzec własnej polityki[8].

W skrócie. *Traktuj odpowiedź AI jak wstępny projekt, a nie gotową decyzję, i weryfikuj każdy fakt, przepis oraz liczbę w wiarygodnym źródle. Nie wpisuj danych osobowych mieszkańców do otwartych narzędzi, a do zadań wrażliwych rozważ polskie i otwarte modele, takie jak PLLuM i Bielik. Ucz się pisać dobre prompty, podając rolę, kontekst i format, oraz oznaczaj treści wygenerowane przez AI tam, gdzie wymaga tego AI Act. Pamiętaj, że za każdą decyzję o skutkach prawnych odpowiada człowiek, nie program.*

Rozdział 8. Obsługa mieszkańców w środowisku cyfrowym

Ten rozdział pokazuje, jak zorganizować pracę zespołu i komunikację z mieszkańcami, wykorzystując narzędzia cyfrowe tak, by obsługa była szybka, uporządkowana i zgodna z RODO.

Cyfrowa organizacja pracy zespołu

Dobra obsługa mieszkańca zaczyna się od porządku w zespole, a ten najłatwiej utrzymać dzięki kalendarzom współdzielonym. Jeden kalendarz – dyżurów – pokazuje godziny pracy poszczególnych okienek, drugi – spotkań – porządkuje wizyty mieszkańców, kalendarz wydarzeń obejmuje sesje rady i konsultacje, a w kalendarzu urlopów umieszcza się dane na temat nieobecności członków zespołu. Widoczność ustawiaj świadomie: wydarzenia otwarte mogą być publiczne, część informacji powinna pozostać wewnętrzna i dostępna tylko dla pracowników, a najbardziej wrażliwe wpisy ograniczone wyłącznie do zespołu.

Tablice zadań

Tablica zadań pokazuje pracę całego zespołu na jednym ekranie. Najpopularniejsze rozwiązania to Trello i Microsoft Planner. Trello jest intuicyjne, oferuje elastyczne etykiety i wiele możliwości integracji, choć ma uboższe opcje raportowania. Microsoft Planner integruje się z Microsoft 365, daje możliwość tworzenia zaawansowanych raportów i synchronizuje się z Outlookiem, jest jednak mniej elastyczny.

Dane, dokumenty, finanse

	Trello	MS Planner
Zalety	intuicyjny, elastyczne etykiety, wiele opcji integracji	integracja z Microsoft 365, zaawansowane raporty, synchronizacja z Outlookiem
Wady	uboższe raportowanie	mniej elastyczny

Na początek utwórz tablicę „Obsługa mieszkańców” z czterema kolumnami: Do zrobienia, W trakcie, Oczekuje i Zakończone. Dodawaj karty zadań z checklistami, przypisuj osoby i terminy oraz ustaw powiadomienia, dzięki czemu nic nie umknie i widać, kto za co odpowiada.

Tablice zadań

Skrzynka zespołowa pod kontrolą

Wspólna skrzynka bywa częstym punktem zapalnym, więc lepiej ją uporządkować. Dobrym początkiem są foldery tematyczne: pilne sprawy do załatwienia w ciągu 24 godzin, sprawy mieszkaniowe, podatki i opłaty, dokumenty i zaświadczenia, skargi i wnioski oraz archiwum. Pracę przyspieszają reguły automatyczne, które sortują wiadomości według nadawcy, oznaczają priorytety, przekierowują korespondencję do odpowiedzialnych osób i archiwizują stare wiadomości. Pomaga też dobrze napisana autoodpowiedź, na przykład: „Dziękujemy za kontakt z Urzędem [nazwa]. Twoja wiadomość została zarejestrowana pod numerem [AUTONUMER]. Odpowiemy w ciągu [X] dni roboczych. W sprawach pilnych: [telefon]. Zespół Obsługi Mieszkańców".

Pamiętaj: wspólna skrzynka nigdy nie powinna pozostawać bez właściciela i jasnych zasad, bo wtedy wiadomości łatwo przepadają między pracownikami.

Rejestr spraw i automatyzacja

Prosty rejestr spraw prowadzony w arkuszu porządkuje pracę i ułatwia raportowanie. Wystarczy tabela z datą, numerem sprawy, nadawcą, tematem, statusem, terminem i osobą odpowiedzialną.

Dane, dokumenty, finanse

Data	Numer	Nadawca	Temat	Status	Termin	Odpowiedzialny
03.09	001/2025	J. Kowalski	zaświadczenie	w trakcie	10.09	A. Nowak

Powtarzalne czynności automatyzuj. Formularz online, na przykład Formularze Google, może samodzielnie zapisywać zgłoszenia do arkusza, a narzędzia typu Power Automate przenoszą dane między systemami. Mniej przepisywania ręcznego oznacza mniej błędów, więc zautomatyzuj przynajmniej rejestrację zgłoszeń i przypomnienia o terminach.

Profesjonalna komunikacja z mieszkańcem

Kanał dobieraj do sprawy. E-mail sprawdza się przy sprawach formalnych, telefon przy pilnych, portal mieszkańca i e-usługi przy załatwianiu spraw online, a media społecznościowe przy informacjach publicznych. Niezależnie od kanału mieszkaniec powinien dostawać spójne doświadczenie, co podkreślono w brytyjskim rządowym Service Standard, którego trzecia zasada wprost zaleca jednolitą obsługę we wszystkich kanałach. Zasada 10. tego samego dokumentu zaleca, by zespół zdefiniował mierniki sukcesu i publikował dane o wydajności.

Praktycznym przełożeniem tych zaleceń jest jeden standard odpowiedzi i wspólny czas reakcji dla całego zespołu oraz przygotowane wcześniej szablony typowych komunikatów: potwierdzenia otrzymania, prośby o uzupełnienie i informacji o terminie. Komunikaty pisz prostym językiem, o którym mowa w Rozdziale 1. Mierz też jakość obsługi za pomocą prostych wskaźników, takich jak czas odpowiedzi, satysfakcja mieszkańców, odsetek spraw rozwiązanych za pierwszym razem oraz dostępność. Projektując formularze i ścieżki obsługi, kieruj się rekomendacją OECD, by usługi budować wokół realnych potrzeb użytkownika i stosować zasadę „pytaj raz", czyli nie wymagać od mieszkańca danych, które urząd już posiada. Zanim przygotujesz formularz, zbadaj potrzeby odbiorców i ogranicz liczbę pól do niezbędnego minimum.

Od 1 stycznia 2026 roku podstawowym sposobem komunikacji podmiotów publicznych z obywatelami i firmami stają się e-Doręczenia, choć sam obowiązek korzystania z nich obejmuje podmioty publiczne, w tym jednostki samorządu, już od 1 stycznia 2025 roku. W praktyce uporządkuj skrzynkę e-Doręczeń: utwórz osobne foldery dla poszczególnych e-usług, ustaw reguły automatycznego kierowania korespondencji do tych folderów i nadaj pracownikom role oraz uprawnienia adekwatne do obsługiwanego zakresu spraw. W całej komunikacji elektronicznej pamiętaj o RODO: ograniczonym dostępie do danych, szyfrowaniu, podstawie przetwarzania oraz prawie mieszkańca do informacji i do usunięcia danych, które w administracji publicznej bywa ograniczone, gdy przetwarzanie wynika z obowiązku prawnego (zob. Rozdziały 2 i 3). Spraw z danymi osobowymi nigdy nie załatwiaj przez prywatne kanały komunikacji.

W skrócie. *Zacznij od porządku w zespole: wspólne kalendarze dyżurów i spotkań oraz tablica zadań z jasnymi statusami i osobami odpowiedzialnymi. Wspólną skrzynkę uporządkuj folderami tematycznymi, regułami automatycznymi i autoodpowiedzią z numerem sprawy, a wszystkie sprawy zapisuj w prostym rejestrze i automatyzuj to, co powtarzalne. Ustal jeden standard odpowiedzi i wspólne wskaźniki jakości dla e-maila, telefonu i e-usług, a komunikaty pisz prostym językiem. Pamiętaj, że obowiązek e-Doręczeń obejmuje podmioty publiczne od 2025 roku, a od 1 stycznia 2026 roku są one podstawowym kanałem kontaktu; pilnuj zgodności z RODO na każdym etapie obsługi.*

Rozdział 9. Case studies. Cyfryzacja w praktyce

Ten rozdział pokazuje na trzech realnych wdrożeniach, co decyduje o powodzeniu projektu cyfrowego w administracji i jak przełożyć cudze doświadczenia na własny urząd.

Po co uczyć się na cudzych wdrożeniach

Najlepsze pomysły na cyfryzację rzadko powstają od zera. Przyglądaj się udanym wdrożeniom i pytaj o trzy rzeczy naraz: jaki problem rozwiązały, jakim narzędziem oraz co właściwie zadecydowało o sukcesie. Taka analiza jest cenniejsza niż gotowa specyfikacja, bo odsłania mechanizm, który da się powtórzyć w innych warunkach. W dalszej części przyglądamy się trzem przykładom – dwóm polskim i jednemu zagranicznemu, a na koniec wyciągamy z nich wspólną metodę doboru rozwiązania.

Case 1 (Polska): e-Recepta

Punktem wyjścia był znany każdemu problem nieczytelnych papierowych recept. Towarzyszyły mu pomyłki w dawkowaniu, trudne do wykrycia interakcje leków oraz codzienna uciążliwość dla pacjentów i aptek. Odpowiedzią stał się centralny system e-recepty prowadzony przez Centrum e-Zdrowia. Pacjent korzysta z niego przez Internetowe Konto Pacjenta, dostępne także w aplikacji mojeIKP, a realizacja w aptece odbywa się na podstawie numeru PESEL i czterocyfrowego kodu. Najważniejsze jest jednak to, że system zamyka obieg danych na linii lekarz–pacjent–apteka, zamiast usprawniać tylko jeden punkt.

Efekt skali mówi sam za siebie. Od 2020 roku wystawiono ponad 2,3 miliarda e-recept, a w samym 2024 roku 521 milionów[1]. Recepty są czytelne, istnieje ich pełny ślad audytowy, a kontrola interakcji leków stała się prostsza. Dobrze zaprojektowane narzędzie nie tylko cyfryzuje papier, ale realnie podnosi bezpieczeństwo obywatela.

Case 2 (Polska): Twój e-PIT

Rozliczenia PIT były przez lata rozproszone między papierem a różnymi systemami, co oznaczało kolejki i błędy przepisywania danych. Usługa Twój e-PIT w e-Urzędzie Skarbowym odwróciła tę logikę: zamiast wymagać od podatnika wypełnienia formularza, państwo przygotowuje gotowe, wstępnie wypełnione zeznanie na podstawie danych od płatników, a obywatel jedynie je akceptuje albo edytuje online. Cały schemat sprowadza się do trzech kroków, czyli logowania, podglądu i akceptacji.

Skutki są wymierne. Za 2025 rok podatnicy złożyli prawie 24 miliony deklaracji elektronicznie i tylko około miliona w formie papierowej, a ponad 35 procent zeznań w usłudze Twój e-PIT zaakceptowano w czasie poniżej pięciu minut[2]. To najlepsza ilustracja zasady „pytaj raz": projektując e-usługę, nie pyta się mieszkańca o dane, które państwo już posiada w rejestrach, lecz pobiera je automatycznie i wstępnie wypełnia formularz, użytkownikowi zostaje wyłącznie sprawdzenie i akceptacja.

Tę samą logikę przenoś na własne formularze: każde pole, które urząd potrafi uzupełnić z rejestru, to pole, o które nie trzeba pytać mieszkańca.

Case 3 (Estonia): Bürokratt

W tradycyjnym modelu to mieszkaniec musi sam znaleźć właściwą usługę, odpowiednią stronę, wymagane dokumenty, opłaty i terminy, a każda z tych przeszkód osobno zniechęca do załatwienia sprawy. Estonia odpowiedziała na to projektem Bürokratt, rządowym asystentem opartym na AI, nazywanym „Siri usług publicznych" i uruchomionym w 2022 roku. Pozwala on uzyskać informacje i uruchomić usługi przez jeden, rozmowny punkt wejścia[3].

Bürokratt jest istotny nie tylko jako ciekawostka, ale jako wskazówka kierunku, w którym zmierza e-administracja. Estończycy zbudowali go na otwartych, wielokrotnie używalnych komponentach typu open source, co obniża koszty i pozwala stopniowo podłączać kolejne instytucje, a od 2026 roku stawiają na spersonalizowane agenty AI oraz interoperacyjność transgraniczną sieci usług. To model, w którym AI staje się warstwą obsługi obywatela nadbudowaną nad istniejącymi rejestrami i e-usługami, a nie kolejnym osobnym systemem (zob. Rozdział 7).

Metoda doboru rozwiązania. Czego uczą te przykłady

Za każdym z opisanych sukcesów stoją te same zasady. Zanim wdrożysz jakiekolwiek narzędzie, przejdź przez krótką listę kontrolną:

1. Czy zamyka obieg danych między wszystkimi stronami, zamiast usprawniać tylko jeden punkt?

2. Czy korzysta z prefillu, czyli wypełnia formularze danymi z rejestrów?

3. Czy automatyzuje walidację na każdym etapie?

4. Czy ma najniższy możliwy próg wejścia dla użytkownika?

5. Czy opiera się na jednym standardzie danych?

6. Czy zapewnia ślad audytowy, który odpowiada na pytania kto, co i kiedy?

Sześć zasad udanego wdrożenia cyfrowego

zamknięty obieg danych

prefill

automatyczna walidacja

niski próg wejścia

jeden standard danych

ślad audytowy

Te zasady mają jednak sens dopiero wtedy, gdy zaczyna się od właściwego problemu, a nie od atrakcyjnego narzędzia. Praktyczny przepis na start jest prosty: wybierz jeden uciążliwy, powtarzalny proces, opisz problem, dobierz proste rozwiązanie, najlepiej z istniejących narzędzi krajowych, przetestuj je na małą skalę, a na końcu zmierz efekt i popraw. ⚠ Najczęstszy błąd to wdrażanie dużego systemu bez testu na małej próbie oraz pomijanie pomiaru efektów, bo bez liczb dotyczących czasu, błędów i satysfakcji nie wiadomo, czy zmiana w ogóle zadziałała.

Warto patrzeć przy tym szerzej niż na własny urząd. Zasada jednorazowości ma już wymiar europejski: w ramach Single Digital Gateway działa System Techniczny „Once-Only" (OOTS), który pozwala urzędom na bezpieczną, automatyczną wymianę urzędowych dokumentów i dowodów między państwami Unii na żądanie obywatela, dzięki czemu mieszkaniec składa dane raz, a urząd sam pozyskuje potrzebne zaświadczenia z innego kraju, zamiast wymagać papierowych odpisów. System ten działa od końca 2023 roku, a Komisja Europejska systematycznie rozwija jego dokumentację techniczną, ułatwiając wdrożenie po stronie krajowych systemów[4]. 🏛 Dla pojedynczego urzędu praktyczny wniosek brzmi tak samo jak w przypadku Twój e-PIT: jeśli dane już gdzieś są, pobierz je, zamiast prosić o nie mieszkańca.

W skrócie. *Zaczynaj od konkretnego problemu, a nie od narzędzia, i sprawdzaj, czy rozwiązanie zamyka obieg danych, korzysta z prefillu i ma niski próg wejścia. Wykorzystuj gotowe rejestry oraz zasadę jednorazowości, tak jak robi to Twój e-PIT, zamiast pytać mieszkańca o dane, które państwo już ma. Nie wdrażaj dużego systemu bez testu na małej próbie i zawsze planuj, jak zmierzysz efekt: czas, liczbę błędów i satysfakcję. Pamiętaj o dostępności, RODO i bezpieczeństwie, a kierunek rozwoju, jak pokazuje estoński Bürokratt, prowadzi ku AI jako wygodnej warstwie obsługi nad istniejącymi e-usługami.*

Najczęstsze pytania urzędnika

Poniżej zebraliśmy pytania, które najczęściej pojawiają się na szkoleniach. Odpowiedzi są krótkie i praktyczne, a po szczegóły odsyłamy do właściwych rozdziałów.

Czy mogę użyć ChatGPT albo innego narzędzia AI do napisania pisma urzędowego?

Tak, ale wyłącznie jako pomoc przy szkicu. Nigdy nie wpisuj do otwartych narzędzi danych osobowych mieszkańców ani informacji niejawnych, a każdą odpowiedź traktuj jak wstępny projekt do sprawdzenia. Za treść pisma odpowiadasz Ty, nie program. Dla zadań wrażliwych rozważ polskie, otwarte modele, takie jak PLLuM czy Bielik (zob. Rozdział 7).

Jak sprawdzić, czy mieszkaniec lub firma ma adres do e-Doręczeń?

Skorzystaj z Bazy Adresów Elektronicznych. Jeśli adresat ma w niej aktywny adres, kieruj korespondencję elektronicznie, a nie listem papierowym (zob. Rozdział 5).

Dostałem podejrzany e-mail. Co robić?

Nie klikaj w link ani załącznik, zgłoś sprawę do działu IT lub inspektora ochrony danych i ostrzeż zespół. Podejrzany SMS przekaż bezpłatnie na numer 8080, a wątpliwy e-mail na adres cert@cert.pl (zob. Rozdział 2).

Czy mDowód jest tak samo ważny jak plastikowy dowód osobisty?

Tak. mDowód w aplikacji mObywatel jest pełnoprawnym dokumentem tożsamości i możesz go honorować przy obsłudze mieszkańca (zob. Rozdział 5).

Mieszkaniec prosi o zaświadczenie, które urząd i tak ma w rejestrze. Czy muszę go o nie prosić?

Najpierw sprawdź, czy potrzebna informacja jest już dostępna w rejestrze, do którego masz dostęp. To zasada „pytaj raz": nie żądaj od obywatela danych, które państwo już posiada (zob. Rozdział 3).

Jak bezpiecznie wysłać dokument z danymi osobowymi?

Wewnątrz urzędu korzystaj z systemu EZD z kontrolą dostępu, a na zewnątrz z ePUAP lub e-Doręczeń i szyfrowanych załączników. Nie używaj do tego prywatnej poczty, komunikatorów ani przypadkowych pendrive'ów (zob. Rozdziały 2 i 6).

Czym różni się anonimizacja od pseudonimizacji?

Anonimizacja nieodwracalnie usuwa dane identyfikujące, więc dane przestają być danymi osobowymi. Pseudonimizacja zastępuje je kodami, ale można ją cofnąć kluczem. Takie dane wciąż pozostają danymi osobowymi chronionymi przez RODO (zob. Rozdział 3).

Co zrobić, gdy w urzędzie dojdzie do ataku ransomware?

Natychmiast odłącz komputer od sieci, nie płać okupu, nie naprawiaj sprzętu samodzielnie i zgłoś sprawę przełożonemu, działowi IT oraz inspektorowi ochrony danych. Przy naruszeniu danych osobowych urząd zgłasza je Prezesowi UODO w ciągu 72 godzin (zob. Rozdział 2).

Jak sprawdzić, czy mój dokument jest dostępny cyfrowo?

Użyj wbudowanej funkcji „Sprawdź dostępność" w edytorze tekstu, zadbaj o właściwy kontrast, hierarchię nagłówków, opisy alternatywne grafik i prosty język. Pomocny bywa też test czytnikiem ekranu, na przykład Narratorem (zob. Rozdział 1).

Gdzie szukać aktualnej, wiarygodnej wiedzy po szkoleniu?

Zacznij od Strefy Uczestnika projektu (cyfryzacja-klaster.pl), Bazy Wiedzy gov.pl oraz komunikatów CERT Polska. Pełny wykaz przydatnych aplikacji i stron znajdziesz w katalogu na końcu książki.

Słowniczek pojęć cyfrowych

Krótkie wyjaśnienia pojęć, które pojawiają się w podręczniku. Definicje celowo są proste, dla szybkiego przypomnienia.

Anonimizacja - Nieodwracalne usunięcie danych identyfikujących, po którym dane przestają być danymi osobowymi.

API - Sposób, w jaki programy „rozmawiają" ze sobą i automatycznie wymieniają dane bez ręcznego przepisywania.

AI Act - Rozporządzenie Unii Europejskiej regulujące wykorzystanie sztucznej inteligencji według poziomu ryzyka.

BAE - Baza Adresów Elektronicznych, czyli rejestr, w którym sprawdzisz, czy dana osoba lub firma ma adres do e-Doręczeń.

CEIDG - Centralna Ewidencja i Informacja o Działalności Gospodarczej, czyli publiczny rejestr przedsiębiorców.

CERT Polska. Zespół reagowania na incydenty komputerowe działający w NASK, do którego zgłaszasz cyberincydenty.

Chmura krajowa - Infrastruktura informatyczna dla sektora publicznego, pozwalająca korzystać z usług bez własnej serwerowni.

Dane otwarte - Informacje publiczne udostępniane bezpłatnie, w formacie maszynowym, do dowolnego ponownego wykorzystania.

Deepfake - Spreparowane nagranie obrazu lub głosu, w którym sztuczna inteligencja podmienia twarz albo głos.

Dezinformacja - Celowe rozpowszechnianie fałszywych informacji, by kogoś wprowadzić w błąd.

Dostępność cyfrowa - Projektowanie treści tak, by mógł z nich skorzystać każdy, także osoby z niepełnosprawnościami.

e-Doręczenia - Elektroniczny odpowiednik listu poleconego za potwierdzeniem odbioru.
ePUAP. Elektroniczna platforma usług administracji publicznej.

EZD - Elektroniczne Zarządzanie Dokumentacją, czyli prowadzenie spraw i akt w postaci cyfrowej.

FIDO2 - Standard bezpiecznego logowania z użyciem klucza sprzętowego, odporny na phishing.

Halucynacja (AI) - Sytuacja, w której model językowy podaje pewnym tonem informację nieprawdziwą, na przykład nieistniejący przepis.

Higiena cyfrowa - Codzienne nawyki, dzięki którym bezpiecznie i zdrowo korzystasz z technologii.

Incydent (bezpieczeństwa) - Zdarzenie zagrażające bezpieczeństwu danych lub systemów, które należy zgłosić.

Interoperacyjność - Zdolność różnych systemów i urzędów do wymiany danych i współdziałania.

IOD - Inspektor Ochrony Danych, osoba czuwająca nad zgodnością przetwarzania danych z RODO.

KSeF - Krajowy System e-Faktur, obowiązkowa od 2026 roku platforma faktur ustrukturyzowanych.

LLM (duży model językowy) - System sztucznej inteligencji przewidujący kolejne słowa, na którym opierają się narzędzia takie jak ChatGPT.

mDowód - Elektroniczny dokument tożsamości w aplikacji mObywatel, równoważny dowodowi plastikowemu.

Menedżer haseł - Program, który generuje i bezpiecznie przechowuje hasła, dzięki czemu pamiętasz tylko jedno główne.

Metadane - Opis zbioru danych mówiący, co zawiera, kiedy powstał i w jakim formacie.

mObywatel - Bezpłatna aplikacja rządowa z dokumentami i e-usługami w telefonie.

Phishing - Próba wyłudzenia danych lub pieniędzy przez podszywanie się pod zaufaną instytucję.

Profil Zaufany - Bezpłatne narzędzie do potwierdzania tożsamości w sieci i składania podpisu zaufanego.

Prompt - Polecenie wydane narzędziu AI; im jest jaśniejsze i bardziej szczegółowe, tym lepszy wynik.

Prosty język - Sposób pisania zrozumiały dla odbiorcy: krótkie zdania, strona czynna, brak zbędnego żargonu.

Pseudonimizacja - Zastąpienie danych identyfikujących kodami; proces odwracalny, dlatego dane pozostają danymi osobowymi.

Ransomware - Złośliwe oprogramowanie, które szyfruje pliki i żąda okupu, a często też kradnie dane.

RODO - Ogólne rozporządzenie o ochronie danych osobowych obowiązujące w całej Unii Europejskiej.

Szyfrowanie - Zabezpieczenie danych tak, by mogła je odczytać tylko osoba uprawniona.

Uwierzytelnianie dwuskładnikowe (2FA) - Logowanie wymagające drugiego potwierdzenia obok hasła, na przykład kodu z aplikacji.

WCAG - Międzynarodowy standard dostępności treści cyfrowych, oparty na zasadach P.O.U.R.

Wyciek danych - Niezamierzone ujawnienie danych osobowych, najczęściej wskutek błędu lub ataku.

CZĘŚĆ KOŃCOWA

Zakończenie. Jak uczyć się dalej

Kompetencje cyfrowe to nie cel, lecz droga. Narzędzia i przepisy zmieniają się szybko, dlatego warto stale je odświeżać. Oto, gdzie szukać aktualnej, rzetelnej wiedzy.

- **Strefa Uczestnika projektu,** czyli materiały, ćwiczenia interaktywne i nagrania, zamieszczone pod adresem cyfryzacja-klaster.pl.
- W **Bazie Wiedzy gov.pl** czekają komunikaty, standardy i szkolenia dla administracji (gov.pl/web/baza-wiedzy).
- **GovTech Polska** to inicjatywy i wsparcie cyfryzacji **(gov.pl/web/govtech).**
- **CERT Polska** pod adresem **cert.pl** publikuje aktualne ostrzeżenia o zagrożeniach.

Na koniec. Wybierz z każdego rozdziału jedną rzecz, którą wdrożysz w tym tygodniu. Małe kroki robione regularnie to najlepszy sposób na trwałą zmianę.

Dziękujemy za udział w szkoleniu i życzymy powodzenia w cyfrowej codzienności urzędu!

Katalog przydatnych linków i aplikacji

Tożsamość i usługi obywatela.

Narzędzie	Do czego służy	Adres
Profil Zaufany	Tożsamość cyfrowa, podpis zaufany	pz.gov.pl
mObywatel / mDowód	Dokumenty i e-usługi w telefonie	gov.pl/web/mobywatel
ePUAP	Platforma usług administracji	epuap.gov.pl
e-Doręczenia	Elektroniczna korespondencja urzędowa	gov.pl/web/e-doreczenia
Portal gov.pl	Punkt dostępu do e-usług	gov.pl

Dane, dokumenty, finanse

Narzędzie	Do czego służy	Adres
dane.gov.pl	Otwarte dane publiczne	dane.gov.pl
EZD RP	Elektroniczne zarządzanie dokumentacją	gov.pl/web/ezd-rp
CEIDG	Ewidencja działalności gospodarczej	biznes.gov.pl
KSeF	Krajowy System e-Faktur	gov.pl/web/finanse
Twój e-PIT	Rozliczenie podatku online	podatki.gov.pl/twoj-e-pit
IKP (pacjent.gov.pl)	Internetowe Konto Pacjenta, e-recepta	pacjent.gov.pl

Bezpieczeństwo i ochrona danych

Narzędzie	Do czego służy	Adres
CERT Polska	Zgłaszanie incydentów, ostrzeżenia	incydent.cert.pl · cert.pl
Zgłaszanie phishingowych SMS	Bezpłatny numer	8080
UODO	Ochrona danych osobowych, decyzje	uodo.gov.pl
Have I Been Pwned	Sprawdzenie wycieku danych/hasła	haveibeenpwned.com
Bezpieczne dane	Poradniki bezpieczeństwa	bezpiecznedane.gov.pl

Dostępność, język, AI

Narzędzie	Do czego służy	Adres
Dostępność cyfrowa	Dobre praktyki, deklaracje	gov.pl/web/dostepnosc-cyfrowa
Jasnopis	Pomiar zrozumiałości tekstu	jasnopis.pl
WebAIM / WAVE	Sprawdzanie kontrastu i dostępności	webaim.org · wave.webaim.org
Demagog	Fact-checking	demagog.org.pl
PLLuM	Polski rządowy model językowy	pllum.org.pl
Bielik	Otwarty polski model językowy	bielik.ai

Aneks

A. Źródła i przypisy
Rozdział 1. Dostępność cyfrowa dokumentów

1. Ustawa z dnia 4 kwietnia 2019 roku o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019 poz. 848), isap.sejm.gov.pl.

2. Europejski akt o dostępności (dyrektywa (UE) 2019/882), stosowany od 28 czerwca 2025 roku; Komisja Europejska, „The EU becomes more accessible for all", 2025, https://commission.europa.eu/news-and-media/news/eu-becomes-more-accessible-all-2025-07-31_en.

3. gov.pl, „Jakie są dobre praktyki z zakresu dostępności cyfrowej", gov.pl/web/dostepnosc-cyfrowa (oraz dane o skali trudności w czytaniu).

4. Najwyższa Izba Kontroli, „Dostępność architektoniczna, cyfrowa i informacyjno-komunikacyjna w samorządach" (kontrola 2019–2025), nik.gov.pl.

5. W3C, Web Content Accessibility Guidelines (WCAG) 2.1/2.2, w3.org.

6. Kampania prostego języka: deklaracja prostego języka (2018, MFiPR), program „Prosto z ZUS", poradniki między innymi Poznania i Warszawy, KPRP, KSAP.

7. gov.uk Accessibility blog (Government Digital Service), „Get to WCAG 2.2 faster with the gov.uk Design System", 2024, https://accessibility.blog.gov.uk/2024/01/11/get-to-wcag-2-2-faster-with-the-gov-uk-design-system/.

8. Krajowa Szkoła Administracji Publicznej (KSAP), „Prosty język w administracji – webinar", 2024, https://ksap.gov.pl/ksap/aktualnosci/prosty-jezyk-w-administracji-webinar-1.

9. gov.uk (Department for Education, blog Digital, Data and Technology), „Introducing the DfE Plain Language standard", 2025, https://dfedigital.blog.gov.uk/2025/03/19/introducing-the-dfe-plain-language-standard/

Rozdział 2. Cyberbezpieczeństwo i ochrona danych

1. CERT Polska (NASK), „Raport Roczny 2024": 600 990 zgłoszeń, 103 449 incydentów, wzrost o 62% rok do roku, cert.pl.

2. Zestawienia kar RODO 2025 (łącznie ponad 64 miliony złotych), między innymi dane UODO oraz opracowania branżowe.

3. UODO, kary za naruszenia przy organizacji wyborów korespondencyjnych: Poczta Polska 27 milionów złotych, Minister Cyfryzacji 100 tysięcy złotych, uodo.gov.pl/pl/138/3590; artykuły 32 i 33 RODO.

4. Przykłady ataków na urzędy w 2025 roku: Urząd Miejski w Wadowicach, gmina Obrazów (województwo świętokrzyskie), urząd w Lewinie Kłodzkim; doniesienia CyberDefence24, samorzad.pap.pl oraz komunikaty urzędów.

5. CISA (Cybersecurity and Infrastructure Security Agency, USA), fact sheet „Implementing Phishing-Resistant MFA"; potwierdzone wytycznymi ENISA do dyrektywy NIS2, 2024, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

6. Ministerstwo Cyfryzacji / CERT Polska (NASK), komunikat „Bezpieczne domeny dzięki narzędziu moje.cert.pl", 2025, https://www.gov.pl/web/cyfryzacja/bezpieczne-domeny-dzieki-narzedziu-mojecertpl.

7. Urząd Ochrony Danych Osobowych (UODO), „Poradnik dotyczący naruszeń ochrony danych osobowych" (wersja zaktualizowana), 2025, https://uodo.gov.pl/pl/138/3561.

8. Ustawa o krajowym systemie cyberbezpieczeństwa; zgłaszanie incydentów: CERT Polska (incydent.cert.pl), CSIRT NASK.

Rozdział 3. Zarządzanie danymi i otwieranie danych

1. UODO, „Sprawozdanie z działalności Prezesa UODO w roku 2024", 14 842 zgłoszenia naruszeń; najczęściej błędne adresowanie korespondencji, uodo.gov.pl/pl/138/3857.

2. European Data Protection Board (EROD/EDPB), „Guidelines 01/2025 on Pseudonymisation" (przyjęte na posiedzeniu plenarnym, styczeń 2025), 2025, https://www.edpb.europa.eu/news/edpb-adopts-pseudonymisation-guidelines-and-paves-the-way-to-improve-cooperation-with_en.

3. Decyzje Prezesa UODO wobec podmiotów publicznych (między innymi burmistrz – 40 tysięcy złotych; Główny Geodeta Kraju – 100 tysięcy złotych; sąd rejonowy), uodo.gov.pl.

4. Portal otwartych danych, dane.gov.pl (Ministerstwo Cyfryzacji).

5. Komisja Europejska, rozporządzenie wykonawcze (UE) 2023/138 ustanawiające wykaz zbiorów danych o wysokiej wartości (HVD), EUR-Lex; data rozpoczęcia stosowania 9 czerwca 2024 roku, 2024, https://eur-lex.europa.eu/eli/reg_impl/2023/138/oj/eng.

6. CEEB, Centralna Ewidencja Emisyjności Budynków, GUNB, zone.gunb.gov.pl.

7. UFG, weryfikacja polis OC, ufg.pl.

8. Profil Zaufany, ponad 13 milionów użytkowników (Ministerstwo Cyfryzacji, gov.pl); Krajowe Ramy Interoperacyjności (KRI).

9. UODO, „Poradnik dotyczący naruszeń ochrony danych osobowych" (aktualizacja, Prezes UODO Mirosław Wróblewski), 2025, https://uodo.gov.pl/pl/598/3563.

Rozdział 4. Odporność i higiena cyfrowa urzędnika

1. World Economic Forum, „Global Risks Report 2025", dezinformacja jako najpoważniejsze zagrożenie krótkoterminowe (drugi rok z rzędu), weforum.org.

2. Demagog, „Podsumowanie 2025 roku", 65 procent zweryfikowanych wypowiedzi polityków to fałsz lub manipulacja (wzrost w stosunku do roku poprzedniego o 17 punktów procentowych), demagog.org.pl.

3. CSIRT KNF / CEBRF, ostrzeżenia o „fałszywych inwestycjach" z wykorzystaniem deepfake i wizerunków znanych osób, cebrf.knf.gov.pl, knf.gov.pl.

4. Microsoft, „Work Trend Index", tempo pracy i przerwy w ciągu dnia, microsoft.com.

5. CIOP-PIB, poradnik „Ćwiczenia fizyczne w miejscu pracy"; zasady ergonomii stanowiska, ciop.pl.

6. Ministerstwo Cyfryzacji i NASK, kampania „Nie bądź internetowym trollem" (gov.pl / Baza wiedzy), 2025, https://www.gov.pl/web/baza-wiedzy/nie-pozwol-by-dezinformacja-zmienila-cie-w-trolla--nowa-odslona-kampanii-ministerstwa-cyfryzacji-i-nask.

7. Komisja Europejska, „Code of Practice on Transparency of AI-Generated Content" (artykuł 50 AI Act), 2026, https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content.

8. Gra edukacyjna „Bad News", getbadnews.com/pl.

9. CIOP-PIB, „Organizacja czasu pracy" (serwis ciop.pl), 2024 (zasada 20-20-20 oraz krótkie, częste przerwy zamiast rzadkich i długich), https://www.ciop.pl/CIOPPortalWAR/appmanager/ciop/pl?_nfpb=true&_pageLabel=P300018313355391822 78&html_tresc_root_id=300008690&html_tresc_id=300008711&html_klucz=19558.

Rozdział 5. Aplikacje krajowe i e-administracja

1. Profil Zaufany, ponad 13 milionów użytkowników (Ministerstwo Cyfryzacji, gov.pl).

2. mObywatel/mDowód, „najpopularniejsza aplikacja rządowa w Europie", gov.pl/web/mobywatel, coi.gov.pl.

3. e-Doręczenia, harmonogram obowiązku: podmioty publiczne od 1 stycznia 2025 roku, firmy w KRS od 1 kwietnia 2025 roku, gov.pl/web/e-doreczenia/harmonogram.

4. KSeF, plan wdrożenia (etapy 2026: 1 lutego 2026 roku i 1 kwietnia 2026 roku), gov.pl/web/finanse, Ministerstwo Finansów.

5. Operator Chmury Krajowej (chmura krajowa); EZD; CEIDG (biznes.gov.pl).

6. Ministerstwo Cyfryzacji, serwis gov.pl, artykuł „mObywatel w 2025: Jak aplikacja ułatwia życie przez cały rok", 2025, https://www.gov.pl/web/cyfryzacja/mobywatel-w-2025-jak-aplikacja-ulatwia-zycie-przez-caly-rok.

7. Komisja Europejska, Shaping Europe's digital future, European Digital Identity (EUDI) Regulation; Rozporządzenie (UE) 2024/1183, 2024, https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation.

8. gov.pl, e-Doręczenia, oficjalny harmonogram wprowadzania obowiązku (ustawa z 18 listopada 2020 roku o doręczeniach elektronicznych), 2025, https://www.gov.pl/web/e-doreczenia/harmonogram.

Rozdział 6. Komunikacja w pracy zdalnej

1. Polski Instytut Ekonomiczny (PIE), analizy na temat pracy zdalnej i elastycznych form pracy (2024 rok); raport Ministerstwa Cyfryzacji na temat cyfryzacji administracji (2023 rok).

2. EZD RP, system elektronicznego zarządzania dokumentacją, NASK; integracja z ePUAP i e-Doręczeniami, gov.pl/web/ezd-rp, nask.pl, ezd.gov.pl. Zob. też: Gov.pl / NASK, „Rozwój polskiej e-administracji dzięki EZD RP – podsumowanie roku", 2026, https://www.gov.pl/web/ezd-rp/ (rosnąca liczba jednostek; wdrożenia finansowane z KPO, także w modelu SaaS).

3. RODO (rozporządzenie (UE) 2016/679), artykuły 5, 28, 32.

4. National Cyber Security Centre (NCSC, Wielka Brytania), „How to secure your online meetings", 2026, https://www.ncsc.gov.uk/guidance/how-to-secure-your-online-meetings.

5. Urząd Ochrony Danych Osobowych (UODO), wskazówki „Jak bezpiecznie korzystać z wideokonferencji?" (relacjonowane między innymi przez prawo.pl i ngo.pl), 2024, https://www.prawo.pl/prawo/wideokonferencje-uodo-radzi-uwazac-na-dane-osobowe,500299.html.

Rozdział 7. AI w pracy urzędnika - od teorii do praktyki

1. OpenAI, premiera ChatGPT 30 listopada 2022 roku; tempo wzrostu liczby użytkowników (pierwszy milion w pięć dni), openai.com.

2. PLLuM (Polish Large Language Model), polski rządowy otwarty model językowy rozwijany we współpracy z Ministerstwem Cyfryzacji, gov.pl/web/cyfryzacja, pllum.org.pl, ai.gov.pl.

3. Bielik, otwarty polski model językowy, Fundacja SpeakLeash przy wsparciu superkomputerów Cyfronetu AGH (między innymi Helios, Athena), bielik.ai, agh.edu.pl.

4. Sprawa Mata v. Avianca (USA, 2023), prawnik wykorzystał ChatGPT, który wygenerował nieistniejące wyroki; zakończona karą dyscyplinarną.

5. AI Act, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689; harmonogram stosowania (1 sierpnia 2024 roku, 2 lutego 2025 roku, 2 sierpnia 2025 roku, 2 sierpnia 2026 roku, 2 sierpnia 2027 roku), Komisja Europejska, digital-strategy.ec.europa.eu; artificialintelligenceact.eu.

6. Obowiązek kompetencji w zakresie AI (artykuł 4 AI Act, od 2 lutego 2025 roku) oraz unijne living repository dobrych praktyk AI literacy. Komisja Europejska, „Shaping Europe's digital future", 2025, https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy.

7. Przewodnik po sztucznej inteligencji dla administracji publicznej. Ministerstwo Cyfryzacji, „AI HUB Poland", 2026, https://ai.gov.pl/aktualnosci/przewodnik-dla-administracji-publicznej.

8. Artificial Intelligence Playbook for the UK Government (10 zasad + checklisty). gov.uk, „Government Digital Service (DSIT)", 2025, https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government.

9. PLLuM, polski rządowy model językowy, pllum.org.pl.

10. Bielik, otwarty polski model (SpeakLeash / Cyfronet AGH), bielik.ai.

11. AI w administracji, informacje ogólne, ai.gov.pl.

12. Harmonogram i treść AI Act, artificialintelligenceact.eu.

Rozdział 8. Obsługa mieszkańców w środowisku cyfrowym

1. Moduł szkoleniowy B2 M2 „Praca w ekosystemie cyfrowym, obsługa mieszkańców” (materiały projektu).

2. RODO (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679), zasady przetwarzania danych w komunikacji z mieszkańcami.

3. Ministerstwo Cyfryzacji / Portal gov.pl, e-Doręczenia: „Zmiany w komunikacji elektronicznej od 1 stycznia 2026 roku”, 2025, https://www.gov.pl/web/e-doreczenia/zmiany-w-komunikacji-elektronicznej-od-1-stycznia-2026-roku.

4. Government Digital Service (gov.uk), „Service Standard” (aktualizacja 29 stycznia 2026 roku), 2026, https://www.gov.uk/service-manual/service-standard.

5. OECD, „Good Practice Principles for Public Service Design and Delivery in the Digital Age”, 2022, https://www.oecd.org/en/publications/oecd-good-practice-principles-for-public-service-design-and-delivery-in-the-digital-age_2ade500b-en.html.

Rozdział 9. Case studies. Cyfryzacja w praktyce

1. Centrum e-Zdrowia, „Ponad 2,3 miliarda wystawionych e-recept” (521 milionów w 2024 roku), cez.gov.pl, ezdrowie.gov.pl.

2. Ministerstwo Finansów / KAS, komunikat „Rozliczenie PIT za 2025 rok. Miliony podatników zaufały usłudze Twój e-PIT”, 2026: około 24 miliony deklaracji elektronicznych wobec około miliona papierowych, ponad 35 procent zeznań złożonych w czasie poniżej pięciu minut, https://www.gov.pl/web/finanse/rozliczenie-pit-za-2025-rok-miliony-podatnikow-zaufaly-usludze-twoj-e-pit.

3. Bürokratt, estoński rządowy asystent oparty na AI (RIA), uruchomiony w 2022 roku, ria.ee, e-estonia.com, Komisja Europejska (interoperable-europe).

4. Komisja Europejska (Digital Building Blocks), System Techniczny „Once-Only” (OOTS), Single Digital Gateway; uruchomienie 12 grudnia 2023 roku, dokumentacja techniczna rozwijana w kolejnych wersjach, https://ec.europa.eu/digital-building-blocks/sites/spaces/OOTS/overview.

5. Komisja Europejska, Interoperable Europe / OSOR, „Digital public services based on open source: case study on Bürokratt” (CC BY 4.0); GovInsider o planach Estonii na 2026 rok, 2024, https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/digital-public-services-based-open-source-case-study-burokratt.

Publikacja sfinansowana ze środków Krajowego Planu Odbudowy i Zwiększania Odporności, NextGenerationEU.

Nr projektu KPOD.05.08-IW.06-0089/25-00.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
CENTRUM PROJEKTÓW POLSKA CYFROWA
KLASTER INNOWACJI SPOŁECZNYCH
NEW EUROPE FOUNDATION
INSTYTUT ROŻDZIEŃSKIEGO