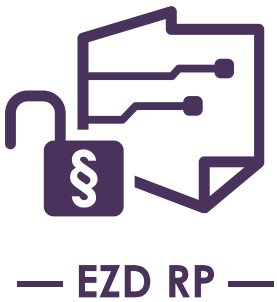

Wymagania w zakresie **przetwarzania danych osobowych**

Warszawa 2023

NASK-PIB
ul. Kolska 12
01–045 Warszawa

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

BNP Paribas Bank Polska Spółka Akcyjna
z siedzibą w Warszawie
ul. Kasprzaka 2, 01-211 Warszawa
Numer konta:
28 1750 0009 0000 0000 0094 9997

www.ezdrp.gov.pl

Wymagania w zakresie przetwarzania danych osobowych w EZD RP

Spis treści

A. Ogólne zasady

1. Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (dalej: NASK) nie jest administratorem EZD RP. NASK udostępnia system jako narzędzie do wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania i rozstrzygania spraw oraz gromadzenia i tworzenia dokumentacji w postaci elektronicznej. Dostarczane oprogramowanie jest „puste". Każda jednostka organizacyjna korzystająca z EZD RP we własnym zakresie decyduje, jakie dane i dokumenty będzie w nim gromadziła.

2. NASK wspiera dwa sposoby wdrażania systemu w podmiotach– jako usługę SaaS EZD RP lub jako instalację na własnej infrastrukturze.

3. Jednostka planująca wdrożenie EZD RP, niezależnie od wybranego modelu, powinna przygotować własną infrastrukturę i procedury organizacyjne w taki sposób, aby umożliwiały one realizację obowiązków określonych między innymi w przepisach i wytycznych obowiązujących dany podmiot. Dotyczy to przede wszystkim:

a) zapewnienia ochrony lokalnej sieci komputerowej lub sieci korporacyjnej za pomocą urządzeń i systemów bezpieczeństwa realizujących funkcje: zapory sieciowej i kontroli

dostępu, szyfrowania połączeń, ochrony przed wirusami i złośliwym oprogramowaniem,

b) stosowania oprogramowania pochodzącego z zaufanych źródeł oraz wdrażania jego aktualnych wersji, w których na bieżąco usuwane są wykryte podatności i luki bezpieczeństwa,
c) zagwarantowania, że dostęp do systemu będą posiadały wyłącznie osoby do tego upoważnione – takie, które w wyznaczonym przedziale czasu realizują zadania w EZD RP.

4. Rozpoczynając korzystanie z usługi chmurowej SaaS EZD RP, poprzez akceptację Regulaminu, określającego odpowiedzialność użytkownika oraz Operatora jako dostawcy usługi, jednostka zawiera umowę. W umowie tej znajdują ustalenia dotyczące powierzenia przetwarzania danych osobowych, ponadto reguluje ona prawa i obowiązki obydwu podmiotów oraz ustanawia cel, jakim jest przechowywanie danych w systemie.
Aby korzystać z systemu w usłudze SaaS EZD RP, jednostka musi zestawić bezpieczne łącze dostępowe IPSec VPN Site-2-Site. Operator usługi chmurowej SaaS EZD RP zastosował rozwiązania infrastrukturalne zapewniające bezpieczeństwo danych poprzez: rozmieszczenie urządzeń i systemów w dwóch niezależnych centrach przetwarzania, wdrożenie rozwiązań wirtualizacyjnych i klastrowych (w szczególności dla podsystemów udostępniających przestrzeń dyskową), cykliczną replikację danych na inne urządzenia, zastosowanie redundancji dla elementów sieciowych i łączy. Dane w systemach produkcyjnych są również objęte procedurami wykonywania kopii bezpieczeństwa zgodnie z parametrami określonymi w Regulaminie. Wykaz środków technicznych i organizacyjnych stosowanych w celu zapewnienia bezpieczeństwa danych osobowych przez operatora usługi SaaS EZD RP stanowi **Załącznik nr 1** do niniejszego dokumentu.

5. Należy podkreślić, że w przypadku świadczenia przez NASK usługi SaaS EZD RP zawierana jest z jednostką organizacyjną umowa powierzenia przetwarzania danych osobowych dla usługi – powierzenie danych następuje w celu ich przechowywania w związku z korzystaniem z usługi, której przedmiotem jest udostępnienie EZD RP drogą elektroniczną w rozumieniu ustawy o świadczeniu usług drogą elektroniczną. W związku z faktem, że przechowywanie jest jednym z „atrybutów" przetwarzania danych osobowych z podmiotami korzystającymi z usługi SaaS EZD RP zostaje zawarta umowa powierzenia ich przetwarzania. Jednostka korzystająca z EZD RP jest administratorem danych osobowych, który ustala cele i sposoby ich przetwarzania oraz decyduje o tym, jakie dane zostaną dodane do systemu. Wykonuje na nich operacje takie, jak:

a) zbieranie,
b) utrwalanie,
c) organizowanie,
d) porządkowanie,

e) przechowywanie,
f) adaptowanie lub modyfikowanie,
g) pobieranie,
h) przeglądanie,
i) wykorzystywanie,
j) ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie,
k) dopasowywanie lub łączenie,
l) ograniczanie, usuwanie lub niszczenie.

6. W przypadku instalacji usługi na własnej infrastrukturze na jednostce zarządzającej tą infrastrukturą spoczywa obowiązek wyboru i zastosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych.

7. Każdy użytkownik EZD RP powinien posiadać nadane przez administratora danych osobowych upoważnienie do ich przetwarzania.

8. Niezależnie od wybranego modelu wdrożenia systemu wykorzystywany sprzęt biurowy powinien być na bieżąco aktualizowany i mieć zainstalowane poprawki bezpieczeństwa.

9. W modelu wdrożenia EZD RP na infrastrukturze lokalnej podmiotu (on-premise), który wymaga przygotowania środowiska pozwalającego na instalację systemu, w tym odpowiednich komponentów (serwera aplikacyjnego, baz danych, repozytoriów dokumentów itd.), zapewnienia sprzętu (serwerów o odpowiedniej mocy obliczeniowej, pamięci operacyjnej, przestrzeni dyskowej, dostępu do sieci LAN itd.) i personelu do jego utrzymania (kopie bezpieczeństwa, utrzymanie systemów, analiza wydajności itd.), to jednostka organizacyjna określa i wdraża środki i sposoby zabezpieczenia infrastruktury i jej komponentów.

10. Każda jednostka organizacyjna korzystająca z EZD RP jako administrator danych osobowych powinna być w stanie udokumentować wdrożenie procedur zapewniających bezpieczeństwo tych danych zgodnie z odpowiednimi przepisami prawa.

B. Wymagania sprzętowe

1. Do prawidłowego działania EZD RP niezbędne jest wykorzystanie stacji roboczych oraz stanowisk obsługi kancelaryjnej o poniżej podanych parametrach.

a) **Stacja robocza – wymagania minimalne:**
   1) system operacyjny: Windows 10 lub 11 z zainstalowanymi aktualizacjami i poprawkami bezpieczeństwa,
   2) procesor: dual core,

3) pamięć RAM: 4 GB,
4) monitor (rozdzielczość ekranu): 1920 × 1080 px (Full HD),
5) przeglądarka internetowa: Microsoft Edge, Mozilla Firefox, Google Chrome, Opera lub Safari z zainstalowanymi aktualizacjami,
6) pakiet biurowy: Microsoft Office 2016 lub inny kompatybilny,
7) aktywne programy zabezpieczające przed wirusami i złośliwym oprogramowaniem,
8) dodatek EZD RP FileMonitor (wersja oprogramowania odpowiadająca wdrożonej wersji systemu),
9) aplikacja umożliwiająca składanie podpisu elektronicznego wraz z nośnikiem lub urządzeniem przechowującym klucze,
10) w przypadku użycia:
    - komputerów przenośnych przeznaczonych do pracy mobilnej – wdrożone oprogramowanie zapewniające bezpieczne połączenie z siecią korporacyjną instytucji (tzw. klient VPN),
    - drukarek kodów kreskowych podłączonych do sieci – zainstalowane na stacji roboczej sterowniki umożliwiające wydruk.

b) Dodatkowe wyposażenie dla stanowisk obsługi kancelaryjnej:

1) zainstalowany dodatek EZD RP QuickScan (wersja odpowiadająca wdrożonej wersji systemu) lub inne oprogramowanie zapewniające prawidłowy eksport danych do EZD RP,
2) skaner (wydajność urządzenia powinna być dostosowana do ilości przetwarzanej dokumentacji, wymagane sterowniki TWAIN i interfejs w języku polskim),
3) czytnik kodów kreskowych wraz z podstawką obsługujący powszechnie stosowane kody kreskowe; wymagana obsługa: Code 128 i Interleaved 2 of 5 (ITF) z możliwością zaprogramowania automatycznego Entera.

c) Drukarka kodów kreskowych

1) podłączona bezpośrednio do stanowiska obsługi kancelaryjnej lub dostępna jako drukarka sieciowa,
2) obsługująca język EPL,
3) umożliwiająca drukowanie na taśmach woskowo-żywicznych i kompatybilnych etykietach (większa żywotność druku) na potrzeby wewnętrzne systemu,
4) umożliwiająca drukowanie na zwykłych etykietach termotransferowych (krótsza żywotność) na potrzeby korespondencji wychodzącej.

C. Struktura organizacyjna i użytkownicy

1. Struktura organizacyjna oraz konta dla użytkowników w podmiocie są tworzone przez administratorów EZD RP wskazanych w danej jednostce organizacyjnej w aplikacji KUiP (Katalog Użytkowników i Podmiotów). Aby utworzyć konto w EZD RP, należy podać następujące dane:

a) imię ,
b) nazwisko,
c) e-mail,
d) login (loginem może być adres e-mail).

2. Zmiany w strukturze organizacyjnej oraz dodawanie i usuwanie użytkowników są wyłącznym uprawnieniem administratora EZD RP wskazanego w podmiocie wdrażającym system.

D. Logowanie się do EZD RP

1. Aby pracownik mógł się zalogować do systemu, administrator EZD RP w danej jednostce organizacyjnej musi utworzyć dla niego konto.

2. Logowanie do systemu odbywa się po podaniu loginu i hasła dostępowego.

3. W EZD RP można ustawić własne hasło dostępowe. Musi ono zawierać przynajmniej osiem znaków, a wśród nich:

a) jedną wielką literę,
b) jedną małą literę,
c) jedną cyfrę,
d) jeden specjalny znak: @, $, !, %, *, # lub ?.

4. Jednostka organizacyjna – przy uwzględnieniu powyższych wymagań – może wskazać, zgodnie z wewnętrzną polityką bezpieczeństwa, własne wytyczne dot. tworzenia przez pracowników haseł dostępowych do systemu (np. w zakresie liczby znaków). Powinny być one opisane w dokumencie wewnętrznym udostępnionym pracownikom.

5. Jeśli pracownik zapomni hasło, może ustawić nowe – przy logowaniu do systemu należy wybrać opcję: **Nie pamiętasz hasła?**

6. Na adres e-mail wskazany podczas zakładania konta dla pracownika zostanie wysłany przez system link, który pozwala na zmianę hasła.

7. Pracownicy, którzy zastępują osoby nieobecne w pracy, powinni korzystać z dostępnej w EZD RP funkcji zastępstw.

E. Uprawnienia w EZD RP

1. Do nadawania w systemie stosownych uprawnień, które pozwalają na wykonywanie określonych czynności, służy moduł **Administracja**.

2. W module **Administracja** można nadać pracownikom odpowiednie uprawnienia. W podręczniku użytkownika w pliku pod tytułem **Przykładowe szablony uprawnień** wskazano ich propozycje. Każda jednostka nadaje je według własnych zasad – na przykład zgodnie z przyjętą w danym podmiocie procedurą. Odpowiednie uprawnienia w EZD RP pozwalają na wykonywanie poszczególnych czynności lub dostęp do określonych informacji i danych.

F. Dostęp do danych i dokumentów w systemie

1. Podstawowa zasada to zapewnienie dostępu do danych i dokumentów użytkownikom, którzy powinni go mieć ze względu na przyjęty w podmiocie obieg dokumentacji (dostęp wynikający ze ścieżki dekretacji).

2. Podstawowy dostęp do spraw, to taki, gdy dostęp do sprawy ma wyłącznie jej właściciel. Aby pracownik mógł z poziomu **Biurko > W toku > Sprawy** oraz **Spisu spraw** wejść do założonej sprawy i aby mógł dodawać do niej dokumenty, musi mieć nadane poniższe uprawnienia:

a) **Sprawy.Lista** na poziomie **Stanowisko**,
b) **Sprawy.Podglad** na poziomie **Stanowisko**,
c) **Sprawy.Edycja** na poziomie **Stanowisko**.

3. Aby pracownik mógł zobaczyć w **Spisie spraw** listę spraw założonych przez inne osoby, należy nadać uprawnienie **Sprawy.Lista** na poziomie **Komórka organizacyjna**.

4. Aby pracownik mógł podejrzeć zawartość spraw prowadzonych przez inne osoby z jego komórki organizacyjnej poprzez **Spis spraw**, należy mu nadać uprawnienie **Sprawy.Podglad** na poziomie **Komórka organizacyjna**.

5. Aby pracownik mógł dodawać dokumenty do sprawy innego pracownika z tej samej komórki organizacyjnej, należy nadać mu uprawnienie **Sprawy.Edycja** na poziomie **Komórka organizacyjna**.

6. Aby pracownik w **Spisie spraw** mógł zobaczyć sprawy prowadzone przez pracowników innych komórek organizacyjnych, należy przy nadawaniu uprawnień wskazać konkretną komórkę lub komórki organizacyjne oraz konkretne uprawnienia (do wyświetlania listy, spraw, zawartości spraw lub do wykonywania operacji na sprawie).

7. Pracownik może również zaprosić innego pracownika jednostki do współdzielenia sprawy – aby mógł wykonać tę czynność, należy mu nadać uprawnienie **Sprawy.Wspoldzielenie**.

8. Podpisywanie dokumentów w EZD RP jest możliwe po nadaniu pracownikowi uprawnienia **Dokumenty.Podpisywanie** na poziomie **Stanowisko.** Po jego nadaniu pracownikowi w **Ustawieniach** w **Profilu użytkownika** pojawi się sekcja umożliwiająca dodanie certyfikatów podpisu kwalifikowanego.

9. Usuwanie dokumentów dodanych do systemu, w tym do spraw, jest możliwe do wykonania przez pracownika. Każda operacja usunięcia odnotowywana jest w historii sprawy. Aby usunąć dokument podpisany podpisem kwalifikowanym, pracownik musi mieć nadane uprawnienie **Dokumenty.UsuwaniePodpisanych** na poziomie **Stanowisko**.

G. Baza kontaktów

1. Baza kontaktów jest zbiorem danych adresowych, który jest częścią właściwej bazy danych zawartej w systemie teleinformatycznym. Ani baza danych, ani będąca jej elementem tabela z bazą adresatów nie ma określonej kategorii archiwalnej.

W EZD RP wpisy do bazy kontaktów tworzą osoby posiadające następujące uprawnienia:

a) **BazaKontaktów.Edycja** – umożliwia dodawanie i edytowanie wpisów w bazie kontaktów;
b) **BazaKontaktów.Usuwanie** – umożliwia usuwanie wpisów z bazy kontaktów.

2. Kontakty przechowywane w bazie kontaktów dzielą się na dwa typy: **Podmiot/Instytucja** oraz **Osoba fizyczna**.

3. W zakresie danych **Podmiotu/instytucji** w systemie mogą być zapisywane następujące dane:

a) nazwa,
b) numer NIP – informacja opcjonalna,
c) numer REGON – informacja opcjonalna,
d) numer KRS – informacja opcjonalna.
e) dane adresowe:

- kod pocztowy,
- miejscowość,
- poczta,
- ulica,
- budynek,
- lokal,
- skrytka pocztowa,
- kraj,
- adres elektroniczny – adres konta klienta na ePUAP,
- adres elektroniczny skrzynki podawczej (nie na ePUAP),
- adres e-doręczeń.

4. W zakresie danych **Osoby fizycznej** w systemie mogą być zapisywane następujące dane:

a) imię,
b) nazwisko,
c) telefon – informacja opcjonalna,
d) PESEL – informacja opcjonalna,
e) dane adresowe:
    - kod pocztowy,
    - miejscowość,
    - poczta,
    - ulica,
    - budynek,
    - lokal,
    - skrytka pocztowa,
    - kraj,
    - adres elektroniczny – adres konta klienta na ePUAP,
    - adres elektroniczny skrzynki podawczej (nie na ePUAP),
    - adres e-doręczeń.

5. Administrator systemu po stronie jednostki korzystającej z usługi EZD RP może poprzez funkcję **Administracja > Zarządzanie metadanymi** wskazać dodatkowe atrybuty dla kontaktu w bazie kontaktów, tj. dla osoby fizycznej lub podmiotu. Dodanie takiego atrybutu, które jest opcjonalne i zależne od jednostki, pozwala na stworzenie dodatkowych pól, które mogą być wskazane jako obowiązkowe do wypełnienia.

H. Wyszukiwarka w EZD RP

1. W EZD RP dostępna jest wyszukiwarka. Domyślnie pozwala ona każdemu użytkownikowi przeszukiwać tylko własne sprawy, dokumenty i pisma. Sprawy, dokumenty i pisma są podlinkowane, a po kliknięciu w link wyświetla się zawartość obiektu.

Wyszukiwarka daje możliwość podglądu akt sprawy pisma wpływającego lub dokumentu, jeśli pracownik ma:

a) dostęp do podglądu akt sprawy (jest jej prowadzącym, ma uprawnienie, dostęp został mu nadany przez prowadzącego),
b) dostęp do dokumentu (jest jego właścicielem lub dokument znajduje się w sprawie, do której ma dostęp, albo w zadaniu, które otrzymał),
c) nadane uprawnienie **WyszukiwanieRozszerzone.Pisma** na poziomie **Stanowisko** pozwalające na wyszukiwanie pism.

2. Wyszukiwanie spraw, dokumentów i pism w całej instytucji możliwe jest po nadaniu uprawnień:

a) **WyszukiwanieRozszerzone.Sprawy** na poziomie **Stanowisko**,
b) **WyszukiwanieRozszerzone.Dokumenty** na poziomie **Stanowisko**,
c) **WyszukiwanieRozszerzone.Pisma** na poziomie **Stanowisko**.

I. Wymagania dotyczące ochrony danych osobowych na etapie archiwizacji dokumentacji

1. W związku z przekazaniem dokumentacji elektronicznej na stan archiwum zakładowego archiwista zakładowy ma zapewniony dostęp do wszystkich pism i danych w tych pismach – podstawą prawną przetwarzania danych osobowych w tym przypadku są przepisy prawa archiwalnego regulujące zasady przechowywania dokumentacji przekazanej na stan archiwum zakładowego wraz z przepisami dotyczącymi jej udostępniania**.**

2. Dostęp do archiwum zakładowego ma tylko i wyłączenie ten pracownik, któremu zostanie nadane uprawnienie **Sprawy.Archiwum** na poziomie **Stanowisko**.

3. Po zarchiwizowaniu dokumentacji (przejęciu na stan archiwum zakładowego) zachowany zostaje dostęp do dokumentów i danych w sprawach dla pracownika prowadzącego sprawę – może on tylko podejrzeć zawartość akt spraw i pism niestanowiących akt spraw, ale nie może wprowadzić żadnych zmian.

4. Za niszczenie dokumentów elektronicznych przechowywanych w EZD RP odpowiada ta jednostka, która system użytkuje, bowiem to ona zgodnie z przepisami Rozporządzenia

Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. z 2006 r., poz. 206, nr 1518) wszczyna procedurę brakowania dokumentacji, która opisana jest w § 9 – 14 ww. rozporządzenia. EZD RP wspiera użytkowników w zakresie:

a) podpowiedzi, dla których spraw minął okres przechowywania,
b) generowania spisu spraw do brakowania,
c) weryfikacji spraw,
d) brakowania dokumentacji elektronicznej.

Należy jednak wskazać, że o brakowaniu danej dokumentacji decyduje zawsze jednostka organizacyjna, która tę dokumentację wytworzyła, po uzyskaniu zgody z właściwego miejscowo archiwum państwowego. EZD RP wykona pewne czynności automatycznie, ale po wskazaniu potrzeby ich wykonania przez pracownika jednostki.

Procedurę przekazywania materiałów archiwalnych stanowiących dokumenty elektroniczne do archiwów państwowych określa wspomniane już powyżej Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. z 2006 r., poz. 206, nr 1518).

J. Wymagania dotyczące ochrony danych osobowych przetwarzanych w systemie w specyficznych przypadkach

1. Paczka administracyjna

W systemie należy przewidzieć możliwość przechowywania informacji o utworzeniu paczki administracyjnej akt danej sprawy, ze wskazaniem momentu jej stworzenia i podmiotu, dla którego została ona wygenerowana/przekazana. Powinna istnieć również możliwość uzupełniania i przekazywania w analogicznej formie dokumentów, które pojawiły się w sprawie już po przekazaniu paczki administracyjnej.

Paczka administracyjna przekazana z innego podmiotu publicznego powinna być przechowywana w systemie w kontekście sprawy (obok akt sprawy), dla której została przekazana, i powinna istnieć zapewniona możliwość jej wizualizacji z uwzględnieniem treści dokumentów oraz metadanych.

Nie jest wykonywana operacja zwrotu paczki administracyjnej do podmiotu macierzystego (w odróżnieniu od akt papierowych), ale trzeba przewidzieć mechanizmy jej usuwania z systemu. Dokumenty z paczki administracyjnej otrzymanej przez podmiot publiczny z innej instytucji nie muszą podlegać przekazaniu do Archiwum Państwowego w ramach paczki archiwalnej tworzonej w podmiocie, który paczkę otrzymał – ponieważ zajmuje się tym instytucja macierzysta, która daną paczkę administracyjną wytworzyła.

2. Postępowanie z pismami błędnie skierowanymi

W przypadku pism błędnie skierowanych, co do których nie ma podstaw do przekazywania wg właściwości (np. wnioski o udostepnienie informacji publicznej z żądaniem danych, których dany organ nie posiada, w związku z czym nie ma obowiązku przekazywania wniosku wg właściwości, wystraczające jest poinformowanie wnioskodawcy o braku posiadania żądanych informacji) po przesłaniu nadawcy pisma stosowanych wyjaśnień/odpowiedzi może pojawić się wątpliwość odnośnie wskazania celu przetwarzania danych. Jest to jednak kwestia proceduralna po stronie jednostki korzystającej z EZD RP, a nie – dotycząca zabezpieczeń w systemie.

Środki techniczne i organizacyjne wykorzystywane w celu zapewnienia bezpieczeństwa danych – zastosowane przez operatora usługi SaaS EZD RP jako podmiot, któremu powierzono przetwarzanie danych osobowych (zgodnie z zawartą umową).

Należy wskazać opis technicznych i organizacyjnych środków (w tym wszelkie stosowne certyfikaty) wdrożonych, aby zapewnić odpowiedni poziom bezpieczeństwa – zarówno przez podmiot przetwarzający, jak i podmioty, którym podpowierzono przetwarzanie danych. Powinny zostać uwzględnione charakter, zakres, kontekst i cel przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych.

Załącznik nr 1

Środki techniczne i organizacyjne wykorzystywane w celu zapewnienia bezpieczeństwa danych – zastosowane przez operatora usługi SaaS EZD RP jako podmiot, któremu powierzono przetwarzanie danych osobowych (zgodnie z zawartą umową).

Lp.	Rodzaj środków	Zastosowanie (tak/nie)	Opis (należy w możliwie szczegółowy sposób opisać środki techniczne i organizacyjne)
1.	**Środki umożliwiające pseudonimizację i szyfrowanie danych osobowych**	tak	Przesyłanie danych z użyciem protokołów szyfrujących (SSL/TLS). Przechowywanie danych – bez szyfrowania, dostęp do nośników, na których znajdują się niezaszyfrowane dane, wyłącznie dla wąskiego grona administratorów operatora EZD RP.

2.	**Środki gwarantujące zdolność do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania**	tak	Infrastruktura zaprojektowana i zaimplementowana z zastosowaniem redundancji (funkcje: failover, klastry, rozproszone systemy plików, redundantne łącza dostępowe), zabezpieczająca przed awarią pojedynczych urządzeń lub usług. Przesyłanie danych z użyciem protokołów szyfrujących (SSL/TLS). Centra przetwarzania spełniające wymagania na poziomie Tier 3 (redundancje zasilania, chłodzenia, ochrona ppoż. i ochrona fizyczna).
3.	**Środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych w razie incydentu fizycznego lub technicznego**	tak	Środki z opisu zawartego w pkt. 2 oraz wdrożone systemy backupowe zapewniające wykonywanie kopii bezpieczeństwa. Replikacja kopii bezpieczeństwa do innego ośrodka przetwarzania.
4.	**Procesy umożliwiające regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania**	tak	Wdrożone mechanizmy monitorowania i alarmowania w przypadku wystąpienia awarii. Okresowe audyty procedur i infrastruktury w ramach wdrożonego systemu zarządzania bezpieczeństwem informacji zgodnego z ISO 27001. Wykonywanie testów poprawności odtwarzania systemu oraz przełączania na ośrodek zapasowy.
5.	**Środki umożliwiające identyfikację i autoryzację użytkowników**	tak	Dostęp do aplikacji oraz interfejsów API wyłącznie po uwierzytelnieniu użytkownika, uwierzytelnianie dwuskładnikowe (login i hasło oraz dostęp do systemu poprzez VPN). Bezpośredni dostęp do infrastruktury serwerowej i przechowującej dane wyłącznie dla wąskiego grona administratorów operatora EZD RP, działania na komponentach technicznych

			wykonywane z użyciem imiennych kont administratorów z zastosowaniem uwierzytelniania dwuskładnikowego (login i hasło oraz VPN/LAN lub klucz uwierzytelniający i hasło oraz VPN/LAN).
6.	**Środki zapewniające ochronę danych w czasie ich przekazywania**	tak	Przesyłanie danych z użyciem protokołów szyfrujących (SSL/TLS). Dostęp do aplikacji oraz interfejsów API wyłącznie po uwierzytelnieniu użytkownika.
7.	**Środki zapewniające ochronę danych w czasie ich przechowywania**	tak	Przechowywanie danych – bez szyfrowania, dostęp do nośników, na których znajdują się niezaszyfrowane dane, wyłącznie dla wąskiego grona administratorów operatora EZD RP. Bezpieczeństwo przechowywania plików/dokumentów tworzonych, modyfikowanych i wyświetlanych na stacjach roboczych użytkowników – zależne od podmiotów użytkujących usługę SaaS EZD RP.
8.	**Środki służące zapewnieniu bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe**	tak	Dostęp do ośrodków przetwarzania i infrastruktury serwerowej wyłącznie dla wąskiego grona administratorów operatora usługi SaaS EZD RP. Procedury ochrony fizycznej lokalizacji operatora i ośrodków przetwarzania zgodne z PN/ISO 27001. Bezpieczeństwo fizyczne miejsc, w których pracują użytkownicy systemu albo są wprowadzane, prezentowane lub modyfikowane dane – zależne od podmiotów użytkujących usługę SaaS EZD RP.
9.	**Środki umożliwiające rejestrowanie zdarzeń**	tak	Włączone mechanizmy zbierania logów na wszystkich komponentach technicznych systemu. Zapisywanie

			w historii akcji wykonywanych przez użytkowników systemu.
10.	**Środki służące do konfiguracji systemu, w tym konfiguracji domyślnej**	tak	Stosowane mechanizmy centralnego zarządzania infrastrukturą i konfiguracją kluczowych komponentów technicznych w oparciu o szablony, centralne polityki zwiększające i zmieniające domyślne konfiguracje uruchomionych usług (hardening).
11.	**Środki dotyczące zarządzania wewnętrznym systemem IT i bezpieczeństwem IT**	tak	Wdrożony system zarządzania konfiguracją i zasobami IT w zakresie infrastruktury SaaS EZD RP oraz wdrożone systemy bezpieczeństwa w zakresie ochrony serwerów i ruchu sieciowego.
12.	**Środki dotyczące certyfikacji / zapewnienia jakości procesów i produktów**	tak	Stosowane praktyki zgodne z PN-ISO/IEC 20000 /ITIL. Wdrożony system zarządzania bezpieczeństwem zgodny z ISO/IEC 27001 m.in. w obszarach wytwarzania oprogramowania EZD RP oraz świadczenia usługi SaaS EZD RP (potwierdzone certyfikatem).
13.	**Środki zapewniające minimalizację danych**	tak	Zakres zbierania i okresy przechowywania danych zgodnie z decyzjami i politykami podmiotu użytkującego usługę SaaS EZD RP.
14.	**Środki zapewniające odpowiednią jakość danych**	tak	Zakres zbierania i okresy przechowywania danych zgodnie z decyzjami i politykami podmiotu użytkującego usługę SaaS EZD RP.
15.	**Środki zapewniające ograniczone zatrzymywanie danych**	tak	Zakres zbierania i okresy przechowywania danych zgodnie z decyzjami i politykami podmiotu użytkującego usługę SaaS EZD RP.

16.	**Środki zapewniające rozliczalność**	tak	Włączone mechanizmy zbierania logów na wszystkich komponentach technicznych systemu. Bezpośredni dostęp do infrastruktury serwerowej i przechowującej dane wyłącznie dla wąskiego grona administratorów operatora EZD RP. Działania na komponentach technicznych wykonywane z użyciem imiennych kont administratorów z zastosowaniem uwierzytelniania dwuskładnikowego (login i hasło oraz VPN/LAN lub klucz uwierzytelniający i hasło oraz VPN/LAN). Dostęp do aplikacji oraz interfejsów API wyłącznie po uwierzytelnieniu użytkownika. Zapisywanie w historii akcji wykonywanych przez użytkowników systemu.
17.	**Środki umożliwiające przenoszenie danych i ich usuwanie**	tak	Operator usługi EZD RP zapewnia możliwość usunięcia danych na żądanie podmiotu użytkującego usługę SaaS EZD RP oraz opcję ich wyeksportowania (celem przeniesienia).
18.	**Inne środki wdrożone przez podmiot przetwarzający**	tak	Uregulowanie zakresu odpowiedzialności podmiotu przetwarzającego w „Umowie powierzenia przetwarzania danych osobowych dla usługi system EZD RP drogą elektroniczną (SaaS EZD RP)".