**DPIA dokonywana na podstawie art. 35 ust. 10 RODO dla projektu ustawy o wyrobach zawierających azbest w ramach czynności przetwarzania związanej z prowadzeniem Bazy Azbestowej:**

Opracowanie/Edytowanie: Izabela Drelich-Sikorska

Ocena/konsultacja: Dariusz Ramocki, IOD

Zatwierdzenie: Aneta Piątkowska

# Kontekst

## Przegląd

#### Ta sekcja pozwala zidentyfikować i przedstawić przedmiot oceny. Należy w sposób syntetyczny opisać rozważane przetwarzanie, jego cele i wyzwania. Należy zidentyfikować administratora danych i ewentualne podmioty przetwarzające. Należy spisać zasady odnoszące się do tego przetwarzania, przydatne lub wymagające przestrzegania, w tym zatwierdzone kodeksy postępowania (art. 40 RODO) oraz certyfikacje w zakresie ochrony danych (art. 42 RODO).

### Jakie przetwarzanie stanowi przedmiot oceny?

*Należy przedstawić syntetyczny opis przetwarzania: jego nazwę, cele, wyzwania (co wniesie), kontekst wykorzystania, itd.*

Analizowane przetwarzanie danych osobowych dokonywane będzie w związku z prowadzeniem przez ministra właściwego do spraw gospodarki Bazy Azbestowej na podstawie przepisów projektowanej ustawy o wyrobach zawierających azbest.

Dane przetwarzane w Bazie Azbestowej pochodzą między innymi z deklaracji dotyczących wyrobów zawierających azbest sporządzanych przez użytkujących wyroby zawierające azbest i składanych do marszałka województwa lub do wójta, burmistrza lub prezydenta miasta (użytkujący, którzy są osobami fizycznymi, niebędący przedsiębiorcami) właściwych ze względu na lokalizację wyrobu zawierającego azbest.

Dane z deklaracji dotyczących wyrobów zawierających azbest będą wprowadzane przez marszałka województwa oraz wójta, burmistrza lub prezydenta miasta do Bazy Azbestowej, którą prowadzi minister właściwy do spraw gospodarki w systemie teleinformatycznym w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557, 1222 i 1717).

Wprowadzanie danych osobowych (imię i nazwisko użytkującego wyroby zawierające azbest będącego osobą fizyczną) nie jest wymagane przez system, co jest związane z zasadą dotyczącą minimalizacji danych. Decyzja o ewentualnym (fakultatywnym) wprowadzeniu tych danych do Bazy Azbestowej będzie należeć do organu wprowadzającego dane. Gromadzenie tych danych osobowych może okazać się potrzebne w przypadku, gdy organ administracji uzna za konieczne dokonanie weryfikacji obecności wyrobów zawierających azbest na terenie odpowiednio gminy lub województwa.

W Bazie Azbestowej będą gromadzone i przetwarzane również dane i informacje dotyczące składowisk odpadów w tym, m.in. nazwa właściciela lub zarządcy składowiska odpadów oraz jego adres i numer telefonu. Dane o składowiskach odpadów będzie wprowadzał i aktualizował marszałek województwa.

Ponadto, integralną część Bazy Azbestowej stanowi: rejestr wykonawców prac oraz rejestr jednostek szkoleniowych. Dane do rejestru wykonawców prac będą wprowadzane oraz aktualizowane przez starostę lub prezydenta miasta na prawach powiatu. Dane do rejestru jednostek szkoleniowych będą wprowadzane oraz aktualizowane przez ministra właściwego do spraw gospodarki.

Cele przetwarzania:

1) gromadzenie i przetwarzanie danych o wyrobach zawierających azbest, w szczególności ilości, rodzaju i jego lokalizacji,

2) monitorowanie ilości unieszkodliwionych i pozostałych do unieszkodliwienia wyrobów zawierających azbest,

3) zapewnienie spójnego systemu gromadzenia i przetwarzania danych o wyrobach zawierających azbest na terenie całego kraju,

4) gromadzenie i przetwarzanie danych o wykonawcach prac oraz o jednostkach szkoleniowych.

### Jakie odpowiedzialności są związane z tym przetwarzaniem?

*Należy opisać zakres odpowiedzialności zaangażowanych stron: administratora danych, ewentualnych podmiotów przetwarzających oraz współadministratorów.*

Minister właściwy do spraw gospodarki jest administratorem danych osobowych przetwarzanych w Bazie Azbestowej.

Minister właściwy do spraw gospodarki:

1) zbiera, przetwarza, przechowuje i zabezpiecza przed utratą informacje gromadzone w Bazie Azbestowej;

2) zapewnia bezpieczeństwo przetwarzanych informacji i dokumentów, które otrzymał w związku z prowadzeniem Bazy Azbestowej, zgodnie z przepisami o ochronie danych osobowych;

3) zapewnia utrzymanie i rozwój technologiczny Bazy Azbestowej.

Integralną częścią Bazy Azbestowej stanowi: rejestr wykonawców prac oraz rejestr jednostek szkoleniowych. Do rejestru wykonawców prac dane będą wprowadzane oraz aktualizowane przez starostę lub prezydenta miasta na prawach powiatu. Dane do rejestru jednostek szkoleniowych będzie wprowadzać oraz aktualizować minister właściwy do spraw gospodarki.

Minister właściwy do spraw gospodarki zleca świadczenie usługi utrzymania i rozwoju systemu Baza Azbestowa podmiotowi zewnętrznemu. Podmiot zewnętrzny będzie podmiotem przetwarzającym, z którym zostanie zawarta umowa powierzenia przetwarzania danych osobowych.

W ramach umowy powierzenia przetwarzania danych osobowych podmiot zewnętrzny będzie miał dostęp do wszystkich danych zgromadzonych w systemie, w tym do danych osobowych wprowadzonych do systemu. Przetwarzanie danych osobowych przez podmiot zewnętrzny będzie obejmowało gromadzenie oraz przetwarzanie w ramach wykonywania czynności utrzymaniowych (m.in. związanych z dziennikami systemowymi, kopiami zapasowymi, bezpieczeństwem, sieci, kontrolą dostępu logicznego) oraz rozwojowych systemu (m.in. związanych z dostępem do danych podczas wprowadzania nowych funkcjonalności do systemu).

### Opis skrócony struktury systemu

Baza Azbestowa to narzędzie informatyczne do gromadzenia i przetwarzania informacji uzyskanych z inwentaryzacji wyrobów zawierających azbest, dostępne dla wszystkich jednostek samorządu terytorialnego.

Na Bazę Azbestową składają się następujące elementy:

* 1. Baza Danych,
  2. System Zarządzania Danymi,
  3. Portal Informacyjny ([www.bazaazbestowa.gov.pl](http://www.bazaazbestowa.gov.pl/)),
  4. GeoPortal GeoAzbest (http://esip.bazaazbestowa.gov.pl/).

Baza Azbestowa wykorzystuje relacyjną bazę danych SQL - PostgreSQL wraz z rozszerzeniem PostGIS do przechowywania informacji o lokalizacji i cechach ewidencjonowanych wyrobów zawierających azbest oraz o użytkownikach Bazy Azbestowej.

Kluczowym elementem Bazy Azbestowej jest przechowywanie informacji o geograficznej lokalizacji zewidencjonowanych wyrobów zawierających azbest. Baza Azbestowa jest przystosowana do przechowywania obrysów działek ewidencyjnych, na których znajdują się wykorzystywane wyroby zawierające azbest. Obrysy działek przechowywane są w formie wielokrotnych wieloboków odwzorowanych w Państwowym Układzie Współrzędnych Geodezyjnych 1992 (EPSG:2180). Powiązanie rekordów opisujących lokalizację z obiektem geodezyjnym następuje na podstawie numeru działki ewidencyjnej.

Do przechowywania danych systemu wykorzystana została baza danych PostgreSQL. Geometria przechowywana jest dzięki rozszerzeniu PostGIS. Współrzędne wszystkich danych geometrycznych przechowywane są w Państwowym Układzie Współrzędnych Geodezyjnych 1992 (EPSG:2180). Znaki kodowane są w systemie UTF-8.

W bazie danych gromadzone są następujące zakresy danych (do czasu wejścia w życie projektowanej ustawy o wyrobach zawierających azbest):

1. Dane słownikowe:
   1. rodzaj miejscowości;
   2. słownik dla nazw pól;
   3. rodzaj gminy;
   4. rodzaj zabudowy;
   5. stopień pilności usunięcia wyrobów zawierających azbest;
   6. typ własności na poziomie gmin;
   7. typ własności na poziomie działek ewidencyjnych;
   8. rodzaj wyrobu azbestowego.
2. Dane z bazy azbestowej:
   1. Dane o lokalizacjach wyrobów;
   2. Dane o wyrobach azbestowych.
3. Dane zagregowane:
   1. Ilość azbestu na poziomie gminy;
   2. Ilość azbestu na poziomie powiatu;
   3. Ilość azbestu na poziomie województwa.
4. Dane zagregowane: Dane geometryczne:
   1. Państwowy Rejestr Granic:
      1. Województwa;
      2. Powiaty;
      3. Gminy.
   2. Państwowy Rejestr Nazw Geograficznych:
      1. Miejscowości:
   3. Obiekty z azbestem:
      1. Działki ewidencyjne;
      2. Budynki.

Jako serwer mapowy wykorzystywany jest GeoServer pracujący jako aplikacja JEE uruchomiona na serwerze aplikacyjnym Tomcat 7.

Na mapie prezentowane mogą być cztery różne grupy danych:

1. Tło mapy pochodzące z zewnętrznych dostępnych w Internecie serwisów mapowych typu WMTS i TMS. Obsługiwane są następujące serwisy:
   1. ortofotomapa udostępniana przez geoportal.gov.pl,
   2. mapa topograficzna udostępniana przez geoportal.gov.pl,
   3. numeryczny model terenu udostępniany przez geoportal.gov.pl,
   4. mapa OpenStreetMap udostępniana przez openstreetmap.org.
2. Dane pochodzące z zewnętrznych dostępnych w Internecie serwisów mapowych typu WMS. Obsługiwane są następujące serwisy:
   1. działki ewidencyjne udostępniane przez geoportal.gov.pl,
   2. obszary chronione udostępniane przez gdos.gov.pl,
   3. budynki udostępniane przez geoportal.gov.pl,
   4. miejscowości i ulice udostępniane przez geoportal.gov.pl,
   5. punkty adresowe udostępniane przez geoportal.gov.pl.
3. Dane geometryczne pozyskane z rządowych baz danych:
   1. podział administracyjny kraju (PRG),
   2. miejscowości (PRNG).
4. Dane geometryczne bazy azbestowej:
   1. działki ewidencyjne z wyrobami azbestowymi,
   2. obrysy budynków z wyrobami azbestowymi,
   3. instalacje rur azbestowo-cementowych.

### Jakie standardy mają zastosowanie?

*Należy wymienić standardy mające zastosowanie w przypadku tego przetwarzania, w szczególności zatwierdzone kodeksy postępowania oraz certyfikaty związane z ochroną danych osobowych.*

Akty prawa obecnie obowiązujące:

1. ustawa z dnia ……………. o wyrobach zawierających azbest,
2. ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902),
3. ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2024 r. poz. 1725),
4. ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2024 r. poz. 1557, 1222 i 1717),
5. ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513, 1222 i 1932) wraz z aktami wykonawczymi,
6. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 r. poz. 773),
7. ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2023 r. poz. 1440).

Regulacje wewnętrzne Ministerstwa Rozwoju i Technologii (dalej: Ministerstwo):

Bezpieczeństwo informacji:

* Polityka Bezpieczeństwa Informacji  w Ministerstwie Rozwoju i Technologii z  4 listopada 2022 r.
* Polityka Bezpieczeństwa Teleinformatycznego i Cyberbezpieczeństwa z 4 maja 2023 r.
* Zarządzenie nr 29 Dyrektora Generalnego Ministerstwa Rozwoju i Technologii  z dnia 5 grudnia 2022 r. w sprawie zasad zarządzania ryzykiem w Ministerstwie Rozwoju i Technologii  – w zakresie szacowania ryzyka w kontekście bezpieczeństwa informacji oraz kontekście bezpieczeństwa przetwarzania danych osobowych, w tym ryzyka naruszenia praw lub wolności osób fizycznych
* Zasady bezpieczeństwa informacji z 3 kwietnia 2024 r.
* Zasady użytkowania sprzętu teleinformatycznego z 23 stycznia 2024 r.
* Zasady zarządzania danymi uwierzytelniającymi z 17 maja 2023 r.
* Zasady projektowania i wytwarzania bezpiecznych systemów oprogramowania z 23 sierpnia 2023 r.
* Zasady zarządzania aktywami teleinformatycznymi z 30 sierpnia 2023 r.
* Procedura zarządzania zdarzeniami i  incydentami związanymi z bezpieczeństwem informacji z 28 czerwca 2023 r.
* Procedura klasyfikacji, oznaczania i postępowania z poszczególnymi grupami informacji z 25 kwietnia 2023 r.
* Procedura zarządzania aktywami w bezpieczeństwie informacji z 19 sierpnia 2024 r.
* Procedura monitorowania, przeglądu, audytu i doskonalenia SZBI z 2 maja 2023 r.

Ochrona danych osobowych:

## a) Polityka Ochrony Danych Osobowych (z 17 października 2024 r.).

## Dane, procesy i aktywa

#### Ta sekcja pozwala zdefiniować i szczegółowo opisać zakres przetwarzania.

### Jakie dane są przetwarzane?

*Należy wymienić dane zbierane i przetwarzane, podając czas ich przechowywania, odbiorców oraz osoby, które mogą mieć do nich dostęp.*

Dane wprowadzane do Bazy Azbestowej pochodzące od użytkujących wyroby zawierające azbest są wprowadzane do systemu przez marszałka województwa oraz wójta, burmistrza lub prezydenta miasta.

W zakres danych wprowadzanych do systemu wchodzą:

1. imię i nazwisko lub firma użytkującego;
2. adres siedziby użytkującego;
3. adres do korespondencji użytkującego;
4. numer telefonu użytkującego (atrybut fakultatywny);
5. numer identyfikacji podatkowej NIP użytkującego (atrybut fakultatywny).

Dane i informacje o składowiskach opadów będzie wprowadzać i aktualizować marszałek województwa. Zakres tych danych i informacji będzie obejmować:

1. podział na składowiska odpadów w fazie eksploatacyjnej i zamknięte, w tym rok zamknięcia;
2. nazwę składowiska odpadów;
3. adres składowiska odpadów;
4. całkowitą pojemność, w tym wolną pojemność (m³);
5. ilość zdeponowanych odpadów zawierających azbest (Mg);
6. kody przyjmowanych odpadów zawierających azbest,
7. nazwę właściciela lub zarządcy;
8. adres właściciela lub zarządcy;
9. numer telefonu właściciela lub zarządcy.

Starosta lub prezydent miasta na prawach powiatu będzie wprowadzać do rejestru wykonawców prac oraz aktualizować następujące dane:

1. status zezwolenia: wydanie, zmiana, cofnięcie lub wygaśniecie zezwolenia;
2. znak decyzji;
3. data wydania decyzji;
4. nazwa organu;
5. imię i nazwisko lub firmę (nazwę);
6. adres miejsca zamieszkania lub siedziby;
7. adres do korespondencji;
8. numer identyfikacji podatkowej NIP lub europejski numer identyfikacji podatkowej;
9. numer w Krajowym Rejestrze Sądowym lub innym właściwym rejestrze prowadzonym w państwie członkowskim Unii Europejskiej;
10. indywidualny numer rejestrowy, o którym mowa w art. 54 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach;
11. wyszczególnienie rodzajów wyrobów zawierających azbest przewidzianych do usuwania lub zabezpieczania;
12. wyszczególnienie rodzajów odpadów zawierających azbest przewidzianych do wytworzenia;
13. oznaczenie przewidywanego okresu wykonywania działalności w zakresie usuwania lub zabezpieczania wyrobów zawierających azbest;
14. zasięg terytorialny działalności wykonawcy prac według województw.

Minister właściwy do spraw gospodarki będzie wpisywać lub aktualizować w rejestrze jednostek szkoleniowych następujące dane:

1. imię i nazwisko lub firmę (nazwę);
2. adres miejsca zamieszkania lub siedziby;
3. adres do korespondencji;
4. numer identyfikacji podatkowej NIP lub europejski numer identyfikacji podatkowej;
5. numer w Krajowym Rejestrze Sądowym lub innym właściwym rejestrze prowadzonym w państwie członkowskim Unii Europejskiej lub w innym państwie wraz z adresem strony internetowej, na której prowadzony jest ten rejestr;
6. numer w rejestrze zezwoleń na świadczenie usług w zakresie szkoleń, prowadzonego w innym niż Rzeczpospolita Polska państwie członkowskim Unii Europejskiej, przedsiębiorców zagranicznych lub innych osób zagranicznych uczestniczących w obrocie gospodarczym na terytorium Rzeczypospolitej Polskiej wraz z adresem strony internetowej, na której prowadzony jest ten rejestr;
7. obszar, na którym będą świadczone usługi w zakresie szkoleń;
8. numer ewidencyjny z rejestru szkół i placówek oświatowych oraz adres strony internetowej, na której prowadzony jest ten rejestr;
9. numer i datę ważności certyfikatu, potwierdzającego wdrożenie systemu zarządzania jakością w zakresie usług szkoleniowych;
10. datę wykreślenia z rejestru jednostek szkoleniowych.

### Jak wygląda cykl życia danych (opis funkcjonalny)?

*Należy uzyskać cykl życia danych (od ich zbierania do ich zniszczenia poprzez przechowywanie, poszczególne etapy przetwarzania, archiwizację, itp.), np. za pomocą schematów przepływu danych (można je dołączyć poniżej) oraz szczegółowego opisu każdego wdrożonego procesu.*

W przypadku danych dotyczących wyrobów zawierających azbest oraz użytkujących wyroby zawierające azbest:

1. Złożenie przez użytkującego wyroby zawierające azbest deklaracji dotyczącej wyrobów zawierających azbest zgodnie z ustawą o wyrobach zawierających azbest (zakres danych i termin złożenia deklaracji) do urzędu gminy lub urzędu marszałkowskiego, właściwego ze względu na miejsce położenia obiektu z wyrobami zawierającymi azbest.

2. Wprowadzanie informacji dotyczących wyrobów zawierających azbest i użytkujących na podstawie otrzymanych deklaracji o wyrobach zawierających azbest do Bazy Azbestowej przez marszałka województwa lub wójta, burmistrza lub prezydenta miasta.

3. W przypadku zmiany danych, złożenie przez użytkującego wyroby zawierające azbest aktualizacji deklaracji dotyczącej wyrobów zawierających azbest zgodnie z ustawą o wyrobach zawierających azbest (zakres danych i termin złożenia deklaracji) do właściwego organu ze względu na miejsce położenia obiektu z wyrobami zawierającymi azbest.

4. Aktualizacja w Bazie Azbestowej danych na podstawie aktualizacji deklaracji dotyczącej wyrobów zawierających azbest.

5. Możliwe przeprowadzenie przez wójta, burmistrza, prezydenta miasta lub marszałka województwa weryfikacji informacji zawartych w Bazie Azbestowej.

7. Dane wprowadzone do systemu nie są z niego usuwane.

8. Dane wprowadzone do systemu nie są archiwizowane.

9. Dane wprowadzone do systemu są przechowywane bezterminowo.

10. Dane osobowe przechowuje się w systemie przez 40 lat, licząc od końca roku kalendarzowego, w którym zostały do niego wprowadzone.

11. Użytkownik wprowadzający dane do systemu może edytować tylko dane wprowadzone z poziomu danego konta użytkownika.

W przypadku danych dotyczących właścicieli lub zarządców składowisk odpadów:

1. Wprowadzenie do Bazy Azbestowej i aktualizacja przez marszałka województwa danych o składowiskach odpadów na podstawie informacji posiadanych z urzędu.

2. Dane wprowadzone do systemu nie są z niego usuwane.

3. Dane wprowadzone do systemu nie są archiwizowane.

4. Dane wprowadzone do systemu są przechowywane bezterminowo.

5. Dane osobowe przechowuje się w systemie przez 40 lat, licząc od końca roku kalendarzowego, w którym zostały do niego wprowadzone.

W przypadku danych dotyczących wykonawców prac:

1. Wykonawca prac przed dniem rozpoczęcia usuwania lub zabezpieczania wyrobów zawierających azbest składa do właściwego starosty lub prezydenta miasta na prawach powiatu wniosek o wydanie zezwolenia na usuwanie lub zabezpieczanie wyrobów zawierających azbest.

2. Wprowadzenie do rejestru wykonawców prac informacji dotyczących ostatecznych decyzji o wydaniu, zmianie, cofnięciu lub wygaśnięciu zezwolenia lub aktualizacja tych informacji przez starostę lub prezydenta miasta na prawach powiatu.

3. Dane wprowadzone do systemu nie są z niego usuwane.

4. Dane wprowadzone do systemu nie są archiwizowane.

5. Dane wprowadzone do systemu są przechowywane bezterminowo.

6. Dane osobowe przechowuje się w systemie przez 40 lat, licząc od końca roku kalendarzowego, w którym zostały do niego wprowadzone.

W przypadku danych dotyczących jednostek szkoleniowych:

1. Złożenie przez jednostkę szkoleniową wniosku o wpis do rejestru jednostek szkoleniowych ministrowi właściwemu do spraw gospodarki na co najmniej 1 miesiąc przed rozpoczęciem działalności szkoleniowej.

2. Minister właściwy do spraw gospodarki wpisuje jednostkę szkoleniową do rejestru jednostek szkoleniowych.

3. Minister właściwy do spraw gospodarki będzie mógł odmówić w drodze decyzji wpisu do rejestru jednostek szkoleniowych.

4. Możliwość zmiany informacji wpisanych do rejestru jednostek szkoleniowych na wniosek złożony ministrowi właściwemu do spraw gospodarki przez jednostkę szkoleniową w terminie 14 dni od dnia, w którym nastąpiła zmiana.

5. Możliwość wykreślenia jednostki szkoleniowej z rejestru jednostek szkoleniowych.

6. Dane wprowadzone do systemu nie są z niego usuwane.

7. Dane wprowadzone do systemu nie są archiwizowane.

8. Dane wprowadzone do systemu są przechowywane bezterminowo.

9. Dane osobowe przechowuje się w systemie przez 40 lat, licząc od końca roku kalendarzowego, w którym zostały do niego wprowadzone.

### Jakie aktywa będą wykorzystywane?

*Należy wymienić wykorzystywane aktywa (systemy operacyjne, aplikacje zawodowe, oprogramowanie biurowe, protokoły, konfiguracje, itd.).*

|  |  |
| --- | --- |
| Oprogramowanie | Zastosowanie |
| ESXi 7.0U3p  ESXi 8.0u2 | System operacyjny serwera dedykowanego |
| Rocky Linux 9.3 | System operacyjny maszyn wirtualnych |
| Apache Tomcat 7 | Serwer Aplikacji |
| Apache 2.4.57 | Serwer Web |
| PostgreSQL 14.12 | Serwer DB |
| Geoserver 2.17.3 | Serwer mapowy |
| Geoserver 2.25.1 | Serwer mapowy |
| Joomla! 3.10.12 | CMS |
| Joomla! 5.1.1 | CMS |
| ClamAV 0.99.2 | Program antywirusowy |

## Podstawowe zasady

## Proporcjonalność i konieczność

#### Ta sekcja pozwala wykazać, że wdrażane są środki niezbędne dla wykonywania praw osób, których dane dotyczą.

### Czy cele przetwarzania są konkretne, wyraźne i prawnie usprawiedliwione?

*Należy uzasadnić, że dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach.*

Cele przetwarzania są konkretne, wyraźne i prawnie usprawiedliwione i wynikają z aktu prawa powszechnie obowiązującego tj. ustawy o wyrobach zawierających azbest.

### Jakie są podstawy prawne, które określają zgodność przetwarzania z prawem?

*Należy przedstawić podstawy prawne przetwarzania (np. zgoda, wykonanie umowy, obowiązek prawnych, żywotne interesy itd.).*

Przetwarzanie na podstawie art. 6 ust. 1 lit. c RODO tj. niezbędności do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z realizacją ustawy o wyrobach zawierających azbest.

### Czy zbierane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych)?

*Należy wyjaśnić, dlaczego poszczególne zbierane dane są niezbędne do celów, w których są przetwarzane.*

Zbierane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych).

Zbierane dane osobowe ograniczone są absolutnie do niezbędnych dla danego celu, unikamy zbierania danych niepotrzebnych, korzystania z danych bez związku z celem oraz nadmiernych skutków dla osób. Zakres zbieranych danych określa ustawa o wyrobach zawierających azbest.

### Czy dane są prawidłowe i w razie potrzeby uaktualniane?

*Należy opisać, w jaki sposób zapewnia się odpowiednią jakość danych.*

Za aktualność danych o wyrobach zawierających azbest odpowiadają użytkujący wyroby zawierające azbest. Obowiązek składania i aktualizacji deklaracji dotyczącej wyrobów zawierających azbest wynika z ustawy o wyrobach zawierających azbest. Za prawidłowość wprowadzania danych do systemu odpowiadają poszczególne organy, zgodnie z ustawą o wyrobach zawierający azbest.

### Jaki jest okres przechowywania danych?

*Należy wyjaśnić, w jaki sposób okres przechowywania poszczególnych danych jest niezbędny dla osiągania celów przetwarzania lub spełnienia wymogów prawnych.*

Dane przechowywane są w systemie bezterminowo.

Dane osobowe przechowuje się w systemie przez 40 lat, licząc od końca roku kalendarzowego, w którym zostały do niego wprowadzone.

# Podstawowe zasady

## Środki ochrony praw osób, których dane dotyczą

#### Ta sekcja pozwala wykazać, że wdrażane są środki niezbędne dla wykonywania praw osób, których dane dotyczą.

### Jak osoby, których dane dotyczą, są informowane o przetwarzaniu?

*Należy opisać, w jaki sposób osoby, których dane dotyczą, są informowane o przetwarzaniu.*

Obowiązek gromadzenia i przetwarzania danych wynika z ustawy o wyrobach zawierających azbest. Wzór deklaracji dotyczącej wyrobów zawierających azbest zostanie określony w rozporządzeniu Ministra Finansów i Gospodarki. Klauzule informacyjne dotyczące przetwarzania danych osobowych zawartych w deklaracjach dotyczących wyrobów zawierających azbest zostaną zamieszczone na odpowiednich stronach Biuletynu informacji Publicznej poszczególnych urzędów obsługujących marszałków województwa oraz wójtów, burmistrzów i prezydentów miast, jak również na stronie Ministerstwa Rozwoju i Technologii (Portal Informacyjny Bazy Azbestowej, prowadzony pod adresem: [www.bazaazbestowa.gov.pl](http://www.bazaazbestowa.gov.pl)).

### Jak uzyskuje się zgody osób, których dane dotyczą?

*Należy opisać procedury uzyskiwania zgody osób, których dane dotyczą.*

Nie dotyczy: przetwarzanie danych osobowych odbywa się na podstawie ustawy o wyrobach zawierających azbest.

### W jaki sposób osoby, których dane dotyczą, mogą wyegzekwować prawo dostępu do danych i prawo do przenoszenia danych?

*Należy opisać procedury umożliwiające osobom, których dane dotyczą, uzyskanie dostępu do swoich danych, ich otrzymanie i przekazanie.*

Dostęp do danych przysługuje na podstawie art. 15 RODO na wniosek złożony do Administratora. Prawo do przenoszenia danych nie przysługuje (art. 20 ust. 1 RODO).

### W jaki sposób osoby, których dane dotyczą, mogą wyegzekwować prawo do sprostowania i prawo do usunięcia danych?

*Należy opisać procedury umożliwiające osobom, których dane dotyczą, sprostowanie i usunięcie swoich danych.*

Użytkujący wyroby zawierające azbest ma obowiązek aktualizować dane, jeśli ulegną zmianie, w ciągu 30 dni od dnia zmiany danych. Prawo do usunięcia danych nie znajduje zastosowania w sytuacji, kiedy przetwarzanie danych osobowych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator (ustawa o wyrobach zawierających azbest).

### W jaki sposób osoby, których dane dotyczą, mogą wyegzekwować prawo do ograniczenia przetwarzania i prawo do sprzeciwu?

*Należy opisać procedury umożliwiające osobom, których dane dotyczą, ograniczenie przetwarzania swoich danych i prawo do sprzeciwu wobec przetwarzania swoich danych osobowych.*

Prawo do ograniczenia przetwarzania przysługuje każdej osobie, której dane przetwarzane są w Bazie Azbestowej na podstawie art. 18 RODO na wniosek złożony do Administratora. Prawo do sprzeciwu nie ma zastosowania, ponieważ przysługuje w przypadku przetwarzania danych w oparciu o prawnie uzasadniony interes Administratora na podstawie art. 6 ust. 1 lit f) RODO, a zatem nie przysługuje podczas przetwarzania danych w Bazie Azbestowej.

### Czy zobowiązania podmiotów przetwarzających zostały jasno określone i zawarte w umowie?

*Dla każdego podmiotu przetwarzającego należy opisać jego zakresy odpowiedzialności (czas trwania, zakres, cel, udokumentowane instrukcje przetwarzania, uprzednia zgoda) i przedstawić stosowne zapisy umów, kodeksy postepowania oraz certyfikacje określające ich zobowiązania.*

Kwestie dotyczące ochrony danych osobowych zostaną zawarte w umowie na świadczenie usług utrzymania i rozwoju systemu Baza Azbestowa oraz w umowie powierzenia przetwarzania danych osobowych.

### W przypadku przekazywania danych poza obszar Unii Europejskiej, czy dane są adekwatnie chronione?

*Dla każdego państwa poza obszarem Unii Europejskiej, w których dane są przechowywane lub przetwarzane, należy podać jego nazwę i zaznaczyć, czy jest uznawane jako oferujące odpowiedni stopień ochrony danych osobowych lub opisać postanowienia dotyczące przekazywania.*

Dane z Bazy Azbestowej nie będą przekazywane poza obszar Unii Europejskiej.

# Ryzyka

## Środki istniejące lub przewidziane

#### Ta sekcja pozwala zidentyfikować środki (istniejące lub przewidziane), które mają wpływ na bezpieczeństwo danych. Poniżej nazwy proszę go krótko opisać.

### Dzienniki systemowe (logi)

*Polityki tworzenia logów zdarzeń i przechowywania pozostawianych zapisów.*

Logi systemu operacyjnego: /var/log

Logi serwera WWW: /var/log/httpd

Logi bazy danych: /var/lib/pgsql/14/data/logs

Logi aplikacyjne ESIP: /opt/tomcat/tomcat-esip/logs

Logi serwera danych przestrzennych: /opt/tomcat/tomcat-geoserver/logs

Logi CMS: /var/log/httpd oraz /var/log/php-fpm

Uwaga ogólna: logi systemowe nie zawierają i nie będą zawierać w swojej treści żadnych danych osobowych. Login użytkownika nie będzie zawierać rzeczywistych danych użytkownika (imię i nazwisko).

### Kopie zapasowe

*Polityki kopii zapasowych i środki pozwalające zapewnić dostępność i/lub integralność danych osobowych, jak również ich poufność (regularność kopii zapasowych, szyfrowanie kanału transmisji danych, test integralności, itd.).*

System Bazy Azbestowej posiada wdrożony system zabezpieczenia przed utratą danych i dostępności serwisów poprzez trzypoziomową kopię bezpieczeństwa. Zastosowany mechanizm pozwala na odzyskanie utraconych danych w wyniku błędu ludzkiego, awarii sprzętowej lub zewnętrznego ataku na system.

Pierwszy poziom kopii bezpieczeństwa jest realizowany w środowisku produkcyjnym systemu Bazy Azbestowej. Aktualne dane z bazy danych są kopiowane co dwadzieścia cztery godziny w obrębie dysku lokalnego maszyny oraz na zewnętrzny serwer FTP. W celu minimalizacji obciążenia systemu oraz uniknięcia wykonywania kopii w czasie aktywności użytkowników w systemie, kopia jest wykonywana pomiędzy godziną 01:00 a 04:00.

Drugi poziom kopii bezpieczeństwa opiera się na lustrzanej kopii środowiska produkcyjnego na niezależnym serwerze. Lustrzana kopia posiada replikowane w czasie rzeczywistym bazy danych systemu Bazy Azbestowej.

Ostatnim poziomem zabezpieczenia, w ramach procedury przywracania sprawności systemu na wypadek wystąpienia katastrofy całkowicie niszczącej dotychczasowe kopie, jest pełna kopia systemu przechowywana na odrębnym serwerze innym niż serwery produkcyjne systemu w innym niezależnym centrum przechowywania danych.

Zastosowano następującą strategię automatycznego tworzenia i testowania kopii zapasowych:

• retencja danych (kopii zapasowych):

o 60 dni (kopia codzienna)

o 90 dni (kopia tygodniowa);

• sposób i częstotliwość wykonywania kopii zapasowych:

o codziennie - kopie baz danych oraz plików systemowych

o raz w tygodniu - pełna kopia systemu;

• częstotliwość odtworzenia i testowania kopii zapasowych:

o raz w tygodniu.

### Polityka ochrony danych osobowych

*Administrator powinien dysponować dokumentacją wyznaczającą formalnie cele i zasady, które będą stosowane dla ochrony danych osobowych (plan działania, regularne przeglądy polityki, ryzyka, itd.) oraz adresatów (użytkownicy, dział IT, itd.).*

Przetwarzanie i ochrona danych osobowych odbywa się w oparciu o przepisy prawa powszechnie obowiązującego oraz regulacje wewnętrzne przyjęte przez ministerstwo obsługujące ministra właściwego do spraw gospodarki. Podmiot przetwarzający w procesie przetwarzania powierzonych danych osobowych zobowiązany jest przetwarzać je w zgodzie z przepisami RODO, wytycznymi wynikającymi z postanowień umowy oraz Polityki ochrony danych osobowych.

### Kontrola dostępu logicznego

*Opis sposobu, w jaki profile użytkowników są definiowane i przydzielane. Należy szczegółowo opisać wdrożone środki uwierzytelniania uściślając, gdy ma to zastosowanie, reguły stosowane dla haseł (minimalna długość, obowiązkowa składnia, okres ważności, liczba nieudanych prób przed blokadą konta, itd.).*

Sposób przechowywania haseł i loginów użytkowników: na serwerze w bazie danych, hasłowane algorytmem *bcrypt.*

Każde hasło musi zawierać minimum 8 znaków, w tym jedną dużą, jedną małą literę i cyfrę.

Zmiana hasła powinna następować nie rzadziej niż co 30 dni.

### Kontrola dostępu fizycznego

*Polityki kontroli dostępu fizycznego do pomieszczeń, w których odbywa się przetwarzanie (wyznaczanie stref, towarzyszenie gościom, noszenie identyfikatorów, zamykane drzwi, itd.).   
Należy wskazać czy wdrożono procedury alarmowania o włamaniu.*

System ulokowany w niezależnym data center bez dostępu dla osób postronnych. Fizyczny dostęp do urządzeń serwerów posiada tylko obsługa techniczna serwerowni. Osoby te nie posiadają za to dostępu do infrastruktury logicznej systemu (odpowiadają tylko za utrzymanie sprzętowe). Kwestie uregulowane w umowie z podmiotem zewnętrznym.

### Bezpieczeństwo sieci

*W zależności od rodzaju sieci, w której odbywa się przetwarzanie (izolowana, prywatna czy internet), administrator powinien wdrożyć odpowiednie systemy ochrony: zapora ogniowa, system wykrywania włamania lub inne urządzenia aktywne lub pasywne, które mają za zadanie zapewnić bezpieczeństwo sieci.*

Zakres wprowadzonych zabezpieczeń w zakresie systemu Bazy Azbestowej jest następujący:

1. Zabezpieczenia gwarantowane przez dostawcę serwera (OVH).
2. System Bazy Azbestowej jest zabezpieczony zaporą ogniową pfSense, zablokowane są wszystkie porty poza koniecznymi do działania systemu.
3. Systemy maszyn wirtualnych są zabezpieczone zaporą systemową firewalld, zablokowane są wszystkie porty poza koniecznymi do działania systemu.
4. Serwisy osiągalne z zewnątrz są zabezpieczone przed atakami typu brute-force za pomocą programu fail2ban.
5. Bazy danych są zabezpieczone w sposób uniemożliwiający połączenie z innych adresów niż konieczne do działania i obsługi Systemu.
6. Zapewniona jest ochrona przed atakami DDoS przez 24 godziny na dobę, niezależnie od ich rodzaju – podwójny system zabezpieczeń: rozwiązania dostawcy serwera + pakiety zabezpieczeń zainstalowane bezpośrednio w środowisku systemu.
7. Wprowadzono dodatkowe zabezpieczenia systemu na poziomie serwera HTTP przeciwko atakom typu DOS w postaci mod\_evasive.
8. Wszystkie pliki wgrywane na serwer przez Portal Informacyjny są skanowane za pomocą programu antywirusowego ClamAV.

Wdrożone standardy zabezpieczeń w zakresie systemu Bazy Azbestowej zapewniają poziom bezpieczeństwa wystarczający, aby uniemożliwić zaistnienie incydentu bezpieczeństwa tj. dokonanie włamania, uzyskania jakiegokolwiek nieautoryzowanego dostępu do serwerów czy baz danych Bazy Azbestowej, który to nieautoryzowany dostęp mógłby zakłócić, przerwać działanie lub spowodować usunięcie, edycję danych.

### Organizacja

*Istnienie struktury organizacyjnej zdolnej do kierowania i nadzorowania ochrony danych osobowych (wyznaczenie IOD, powołanie komitetu monitorującego, itd.)*

W Ministerstwie został wyznaczony Inspektor Ochrony Danych.

W Ministerstwie ustanowiono Politykę ochrony danych osobowych.

### Nadzór

*Wprowadzenie środków pozwalających uzyskiwać całościową i aktualną wizję stanu ochrony danych i zgodności z RODO (kontrola zgodności czynności przetwarzania, celów i wskaźników, zakresy odpowiedzialności, itd.).*

Umowa z wykonawcą zewnętrznym gwarantuje bieżące dostosowywanie zgodności przetwarzania z obowiązującymi przepisami. Umowa obejmuje prawo do przeprowadzenia audytu prawidłowości wykonania umowy, w tym w zakresie oceny poziomu bezpieczeństwa systemu, szczelności i odporności na nieupoważnione ingerencje. IOD prowadzi audyty zgodności przetwarzania w zakresie wypełniania przez Administratora obowiązków informacyjnych, jest monitorowana aktualność RCP.

### Zarządzanie pracownikami

*Wprowadzenie planu wyznaczającego* ***sposoby uświadamiania*** *podejmowane w stosunku do nowego pracownika oraz procedury opisującej* ***środki podejmowane w stosunku do osób odchodzących z pracy.***

Pracownicy Departamentu MRiT nadzorującego utrzymanie i rozwój Bazy Azbestowej mają dostęp do szkoleń z zakresu bezpieczeństwa informacji, ochrony danych osobowych w ramach indywidualnego programu rozwoju (IPRZ) prowadzonego przez Ministerstwo, jak również do szkoleń realizowanych w tym zakresie w Ministerstwie.

### Zarządzanie naruszeniami ochrony danych osobowych

*Wprowadzenie operacyjnej struktury organizacyjnej pozwalającej wykrywać i obsługiwać zdarzenia, które mogą mieć wpływ na prawa i wolności osób, których dane dotyczą (określenie odpowiedzialności, plan reagowania, klasyfikacja naruszeń, itd.).*

Zarządzanie naruszeniami ochrony danych osobowych regulowane jest w:

• Polityce Ochrony Danych Osobowych (z 8 lipca 2022 r.).

• Procedurze zarządzania zdarzeniami i incydentami związanym z bezpieczeństwem informacji (z 28 czerwca 2023 r.)

### Zarządzanie ryzykiem

*Polityka wyznaczająca proces kontroli ryzyka, że czynności przetwarzania w organizacji mogą wpłynąć na prawa i wolności osób, których dane dotyczą (rejestr czynności przetwarzania danych osobowych, danych, nośników, ocena ryzyka, ustalenie istniejących i planowanych środków, itd.).*

Okresowo wykonywane są analizy ryzyka, weryfikacje dotychczasowych analiz wraz z ewaluacją zidentyfikowanych ryzyk, bądź wprowadzeniem nowych – zgodnie z obowiązującymi regulacjami MRiT w tym zakresie. Analiza ryzyka odbywa się zgodnie z zasadami zarządzania ryzykiem w oparciu o przyjętą metodykę, również w kontekście bezpieczeństwa informacji i bezpieczeństwa przetwarzania danych osobowych.

### Ochrona przed nieosobowymi źródłami ryzyka

*Środki wdrożone w celu ograniczenia lub uniknięcia nieosobowych źródeł ryzyka (zjawiska pogodowe, pożar, zalanie, wypadki wewnętrzne lub zewnętrzne, zwierzęta, zasilanie, itd.), które mogą naruszyć dane osobowe.*

Umowa z wykonawcą zewnętrznym na świadczenie usługi utrzymania i rozwoju Bazy Azbestowej gwarantuje ochronę przed nieosobowymi źródłami ryzyka, m.in. pożar, zalanie.

### Zabezpieczenie sprzętu (hardware)

*Środki wdrożone w celu ograniczenia prawdopodobieństwa, że właściwości sprzętu (serwerów, stacji roboczych, urządzeń mobilnych, peryferyjnych, przełączników, itd.) zostaną wykorzystane w celu naruszenia danych osobowych (spis inwentaryzacyjny, partycjonowanie, redundancja sprzętowa, ograniczenie dostępu, itd.).*

Umowa z wykonawcą zewnętrznym na świadczenie usługi utrzymania i rozwoju Bazy Azbestowej gwarantuje zabezpieczenie sprzętu.

System ulokowany jest w niezależnym data center bez dostępu dla osób postronnych. Fizyczny dostęp do urządzeń serwerów posiada tylko obsługa techniczna serwerowni. Osoby te nie posiadają za to dostępu do infrastruktury logicznej systemu (odpowiadają tylko za utrzymanie sprzętowe).

System zabezpieczony został poprzez zastosowanie lustrzanego środowiska produkcyjnego ulokowanego na odrębnym serwerze fizycznym w odrębnym data center. Dane są replikowane z serwera produkcyjnego do serwera lustrzanego w czasie rzeczywistym.

Dane przechowywane są na dyskach NVMe z zastosowaniem SOFT RAID 1.

### Monitorowanie aktywności sieci

*Środki wdrożone w celu umożliwienia wczesnego wykrywania incydentów dotyczących danych osobowych i analizy ruchu w sieciach (sieci kablowe, Wi-Fi, radiolinie, światłowody, itd.) w czasie rzeczywistym w celu wykrycia aktywności sugerującej cyberatak.*

Umowa z wykonawcą zewnętrznym na świadczenie usługi utrzymania i rozwoju Bazy Azbestowej swoim zakresem obejmuje ochronę przed atakami z sieci Internet oraz możliwość szybkiego reagowania na incydenty. Ponadto Wykonawca prowadzi rejestr incydentów bezpieczeństwa.

Zakres wprowadzonych zabezpieczeń w zakresie systemu Bazy Azbestowej jest następujący:

1. Zabezpieczenia gwarantowane przez dostawcę serwera (OVH).
2. System Bazy Azbestowej jest zabezpieczony zaporą ogniową pfSense, zablokowane są wszystkie porty poza koniecznymi do działania systemu.
3. Systemy maszyn wirtualnych są zabezpieczone zaporą systemową firewalld, zablokowane są wszystkie porty poza koniecznymi do działania systemu.
4. Serwisy osiągalne z zewnątrz są zabezpieczone przed atakami typu brute-force za pomocą programu fail2ban.
5. Bazy danych są zabezpieczone w sposób uniemożliwiający połączenie z innych adresów niż konieczne do działania i obsługi Systemu.
6. Zapewniona jest ochrona przed atakami DDoS przez 24 godziny na dobę, niezależnie od ich rodzaju – podwójny system zabezpieczeń: rozwiązania dostawcy serwera + pakiety zabezpieczeń zainstalowane bezpośrednio w środowisku systemu.
7. Wprowadzono dodatkowe zabezpieczenia systemu na poziomie serwera HTTP przeciwko atakom typu DOS w postaci mod\_evasive.
8. Wszystkie pliki wgrywane na serwer przez Portal Informacyjny są skanowane za pomocą programu antywirusowego ClamAV.

Wdrożone standardy zabezpieczeń w zakresie systemu Bazy Azbestowej zapewniają poziom bezpieczeństwa wystarczający, aby uniemożliwić zaistnienie incydentu bezpieczeństwa tj. dokonanie włamania, uzyskania jakiegokolwiek nieautoryzowanego dostępu do serwerów czy baz danych Bazy Azbestowej, który to nieautoryzowany dostęp mógłby zakłócić, przerwać działanie lub spowodować usunięcie, edycję danych.

### Bezpieczeństwo stron www

*Wdrożenie rekomendacji dotyczących bezpieczeństwa stron www*.

Umowa z wykonawcą zewnętrznym na świadczenie usługi utrzymania i rozwoju Bazy Azbestowej obejmuje swoim zakresem zapewnienie bezpieczeństwa stron www.

Całość komunikacji na stronach www systemu Baza Azbestowa odbywa się za pośrednictwem szyfrowanego połączenia (protokół https).

### Zarządzanie stacjami roboczymi

*Środki wdrożone na stacjach roboczych (automatyczna blokada, regularne aktualizacje, konfiguracja, bezpieczeństwo fizyczne, itd.) w celu ograniczenia prawdopodobieństwa, że właściwości oprogramowania (systemy operacyjne, aplikacje biznesowe, oprogramowanie biurowe, parametryzacje itp.) zostaną wykorzystane do naruszenia danych osobowych.*

Stacje robocze pracowników Ministerstwa administrowane są zgodnie z zasadami przyjętymi i nakładanymi na użytkowników przez Departament Gospodarki Cyfrowej.

### Zwalczanie złośliwego oprogramowania

*Środki ochrony wdrożone na stacjach roboczych i serwerach w celu ich ochrony przed złośliwym oprogramowaniem w trakcie korzystania z sieci słabo zabezpieczonych.*

Umowa z wykonawcą zewnętrznym na świadczenie usługi utrzymania i rozwoju Bazy Azbestowej obejmuje swoim zakresem zwalczanie złośliwego oprogramowania (informacje w podsekcji **Bezpieczeństwo sieci).**

### Zabezpieczenie eksploatacji

*Polityki pozwalające ograniczyć prawdopodobieństwo i istotność ryzyk dotyczących narzędzi wykorzystywanych w trakcie eksploatacji (należy dokumentować procedury eksploatacyjne, wykaz i aktualizację oprogramowania i materiałów, korygowanie podatności, duplikowanie danych, ograniczenie dostępu fizycznego do sprzętu, itd.).*

Umowa zawarta z wykonawcą zewnętrznym na świadczenie usługi i rozwoju Bazy Azbestowej obejmuje swoim zakresem zapewnienie aktualizacji systemu i utrzymanie odpowiedniego poziomu bezpieczeństwa wykorzystywanego oprogramowania (podsekcja **Zabezpieczenie sprzętu (hardware)).**

### Minimalizacja danych osobowych

*Można wykorzystać następujące sposoby: filtrowanie i usunięcie, ograniczenie wrażliwości poprzez konwersję, ograniczenie charakteru identyfikacyjnego danych, ograniczenie gromadzenia danych, ograniczenie dostępu do danych*.

Zakres danych przetwarzanych w systemie jest ograniczony do danych wymaganych przez ustawę o wyrobach zawierających azbest. Nieodpłatny dostęp do informacji dotyczących wyrobów zawierających azbest, użytkujących, składowisk odpadów oraz informacji objętych rejestrem wykonawców oraz rejestrem jednostek szkoleniowych przysługiwać będzie:

1. wójtom, burmistrzom lub prezydentom miast;
2. starostom lub prezydentom miast na prawach powiatach;
3. marszałkom województw.

Ponadto, ww. informacje, z wyjątkiem dotyczących użytkujących, będą udostępnione nieodpłatnie za pośrednictwem strony internetowej wskazanej pod adresem elektronicznym określonym w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw gospodarki, w celu umożliwienia potwierdzenia prowadzenia przez wykonawcę prac lub jednostkę szkoleniową działalności zgodnie z przepisami ustawy i w zakresie koniecznym do realizacji tego celu.

Dostęp do informacji zawartych w Bazie Azbestowej pochodzących z terenu całego kraju na potrzeby postępowania podatkowego, kontroli celno-skarbowej, kontroli podatkowej, czynności sprawdzających oraz audytu będą mieć także, na wniosek, organy Krajowej Administracji Skarbowej.

### Archiwizacja

*Polityka przechowywania i zarządzania archiwami elektronicznymi zawierającymi dane osobowe mającymi zagwarantować jakość tych danych, w tym prawną, podczas całego wymaganego okresu (deponowanie, składowanie, migracja, dostępność, eliminowanie, polityka archiwizacji, ochrona poufności, itd.).*

Dane przechowywane są w systemie bezterminowo.

Dane osobowe przechowuje się w systemie przez 40 lat, licząc od końca roku kalendarzowego, w którym zostały do niego wprowadzone.

### Szyfrowanie

*Środki wprowadzone w celu* ***zapewnienia poufności danych*** *przechowywanych (w bazie danych, w plikach prostych, w kopiach, itp.) jak również procedury zarządzania kluczami szyfrującymi (tworzenie, przechowywanie, modyfikowanie w razie podejrzenie kompromitacji, itd.).   
Należy szczegółowo opisać środki szyfrowania stosowane przy przepływach danych (VPN, TLS, itd.) następujących w trakcie przetwarzania.*

Całość komunikacji na stronach www systemu Baza Azbestowa odbywa się za pośrednictwem szyfrowanego połączenia (protokół https).

### Zabezpieczenie dokumentów papierowych

*Polityki opisujące, jak w trakcie przetwarzania drukowane, przechowywane, niszczone i wymieniane są dokumenty papierowe zawierające dane osobowe.*

Zasady postępowania z dokumentami papierowymi (deklaracje) są określone w ustawie o wyrobach zawierających azbest.

Wójt, burmistrz lub prezydent miasta zapewnia bezpieczeństwo przetwarzanych informacji oraz deklaracji dotyczących wyrobów zawierających azbest, które stanowią podstawę wprowadzenia do Bazy Azbestowej danych, zgodnie z przepisami o ochronie danych osobowych.

Marszałek województwa zapewnia bezpieczeństwo przetwarzanych informacji oraz deklaracji dotyczących wyrobów zawierających azbest, które stanowią podstawę wprowadzenia do Bazy Azbestowej danych, zgodnie z przepisami o ochronie danych osobowych.

### Umowa powierzenia przetwarzania

*Dane osobowe ujawnione podmiotom przetwarzającym lub zarządzane przez nich powinny korzystać z odpowiednich gwarancji.* ***Należy korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje*** *(w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby). Należy wymagać od usługodawcy ujawnienia swojej polityki bezpieczeństwa systemów informatycznych.  
Należy podjąć działania (audyty bezpieczeństwa, oględziny instalacji, itd.), które pozwolą* ***zapewnić skuteczność gwarancji oferowanych przez podmiot przetwarzający w sprawie ochrony danych i je dokumentować. Te gwarancje obejmują m.in.:  
- szyfrowanie danych w zależności od ich wrażliwości lub w przypadku braku szyfrowania istnienie procedur gwarantujących, że usługodawca nie ma dostępu do danych, które zostały mu powierzone  
- szyfrowanie transmisji danych (np. połączeń typu HTTPS, VPN, itd.)  
- gwarancje dotyczące ochrony sieci, logów systemowych (dzienniki, ścieżki audytowe), zarządzania upoważnieniami, uwierzytelnianiem, itd.  
Należy opracować taką umowę z podmiotami przetwarzającymi, która określa m.in. przedmiot, czas trwania, cel przetwarzania i zobowiązania stron oraz upewnić się, że zawiera w szczególności postanowienia ustalające:  
- ich zobowiązania w kwestii poufności powierzonych danych osobowych  
- minimalne wymogi dotyczące uwierzytelniania użytkowników  
- warunki zwrotu i/lub zniszczenia danych na końcu umowy  
- zasady zarządzania incydentami i ich notyfikacji. Te zasady powinny obejmować zawiadomienie administratora w przypadku wykrycia naruszenia bezpieczeństwa lub incydentu bezpieczeństwa i to w najkrótszym możliwym czasie w przypadku naruszenia ochrony danych osobowych  
- W przypadku korzystania z dostawcy cloud computing należy:  
1. dokładnie zidentyfikować dane i czynności przetwarzania, które zostaną przeniesione do chmury ;  
2. określić swoje wymagania dotyczące bezpieczeństwa technicznego i prawnego;  
3. przeprowadzić analizę ryzyka w celu identyfikacji odpowiednich środków bezpieczeństwa;  
4. zidentyfikować rodzaj chmury właściwy dla przewidywanego rodzaju przetwarzania;  
5. wybrać usługodawcę wykazujący się wystarczającymi gwarancjami;  
6. dokonać przeglądu wewnętrznej polityki bezpieczeństwa;  
7. śledzić zmiany w czasie.***

Kwestie ochrony danych osobowych zostały uregulowane w umowie z wykonawcą zewnętrznym oraz w ustawie o wyrobach zawierających azbest.

# Ryzyka

## Nieupoważniony dostęp do danych

#### Należy dokonać analizy przyczyn i konsekwencji nieupoważnionego dostępu do danych i oszacować jego istotność oraz prawdopodobieństwo.

### Jakie mogą być główne skutki dla osób, których dane dotyczą, jeżeli ryzyko się zdarzy?

*Należy przedstawić potencjalne skutki.*

W Bazie Azbestowej gromadzone są przede wszystkim dane o lokalizacji wyrobów zawierających azbest, przy czym większość wyrobów zawierających azbest stanowi pokrycie dachów. Dane lokalizacyjne same w sobie nie identyfikują osób fizycznych. Nawet w przypadku jednak nieupoważnionego dostępu do tych danych, ujawnienie imienia i nazwiska oraz lokalizacji budynku, nie wpłynie znacząco na zwiększenie ryzyka w zakresie ochrony danych osobowych użytkowników tych wyrobów azbestowych będących osobami fizycznymi, w tym zwłaszcza na ich bezpieczeństwo finansowe. Informacje te, bez dodatkowych szczegółowych danych, takich jak, np. numer PESEL, numer dowodu osobistego, czy innych informacji finansowych, nie są wystarczające, by doszło do działań mogących zagrozić bezpieczeństwu finansowemu takiej osoby.

Dane dotyczące właścicieli lub zarządców składowisk odpadów są umieszczane w Bazie danych o produktach i opakowaniach oraz o gospodarce odpadami (BDO).

Ponadto, integralną część Bazy Azbestowej będzie stanowić także: rejestr wykonawców prac oraz rejestr jednostek szkoleniowych.

Należy wskazać, że dane przedsiębiorców będących osobami fizycznymi są umieszczane w publicznym rejestrze: CEIDG.

Zakres danych dotyczący wykonawców prac, jak również jednostek szkoleniowych zawarty w Bazie Azbestowej nie będzie obejmował takich danych jak: PESEL, czy data urodzenia. Przede wszystkim w obu przypadkach będą przetwarzane m.in. takie dane jak: imię i nazwisko, adres miejsca zamieszkania oraz adres do korespondencji. Można przyjąć, że w przypadku nieupoważnionego dostępu do tych danych w Bazie Azbestowej ryzyko dla ww. podmiotów będzie ograniczone. Ujawnienie tych danych może prowadzić np. do niepożądanego kontaktu, wysyłania niechcianych wiadomości (spam) lub prób wyłudzenia informacji.

### Jakie są główne zagrożenia, które mogą doprowadzić do zdarzenia się ryzyka?

*Należy przedstawić zagrożenia.*

Brak prawidłowego działania Bazy Azbestowej, atak hackerski przez osobę nieupoważnioną (włamanie), nieumyślny wyciek danych w wyniku błędu użytkownika Bazy Azbestowej, błąd w zakresie nadawania uprawnień, ujawnienie danych niepodlegających udostępnieniu (nieprawidłowe przechowywanie danych dostępowych do systemu).

### Jakie są źródła ryzyka?

*Należy źródła ryzyka.*

Incydent lub szkoda w data center (przerwa w zasilaniu, pożar, zalanie), źródła osobowe wewnętrzne - nieumyślne działanie pracownika, źródła osobowe zewnętrzne - osoba trzecia, mająca złe zamiary, haker obierający za cel naruszenie wizerunku Ministerstwa, upoważniony podmiot trzeci wykorzystujący swój dostęp uprzywilejowany do bezprawnego dostępu do informacji.

### Które ze zidentyfikowanych środków pozwoli zająć się ryzykiem?

*(Proszę wymienić z katalogu wcześniej zidentyfikowanych środków w zakładce „Środki istniejące lub przewidziane”.*

Dzienniki systemowe (logi), kopie zapasowe, polityka ochrony danych osobowych, kontrola dostępu logicznego, kontrola dostępu fizycznego, bezpieczeństwo sieci, ochrona przed nieosobowymi źródłami ryzyka, zabezpieczenie sprzętu (hardware), monitorowanie aktywności sieci, zabezpieczenie eksploatacji.

### Jaka jest szacowana istotność ryzyka, w zależności od potencjalnych skutków i  przewidzianych środków?

*Skala: Pomijalne – Ograniczone – Poważne - Maksymalne*

Ograniczone.

Uzasadnienie: Zastosowane środki powodują, że prawdopodobieństwo należy uznać za ograniczone.

### Jakie jest szacowane prawdopodobieństwo ryzyka, szczególnie w odniesieniu do zagrożeń, źródeł ryzyka i przewidzianych środków?

*Skala: Pomijalne – Ograniczone – Poważne – Maksymalne*

Pomijalne.

Uzasadnienie: Zastosowane środki powodują, że prawdopodobieństwo należy uznać za pomijalne.

# Ryzyka

## Niepożądana modyfikacja danych

#### Należy dokonać analizy przyczyn i konsekwencji niepożądanej modyfikacji danych i oszacować jego istotność oraz prawdopodobieństwo.

### Jakie mogą być główne skutki dla osób, których dane dotyczą, jeżeli ryzyko się zdarzy?

*Należy przedstawić potencjalne skutki.*

Baza Azbestowa opiera się na lokalizacji wyrobów zawierających azbest. Niepożądana modyfikacja danych w zakresie lokalizacji wyrobów zawierających azbest może wpłynąć na prawa i wolności osób fizycznych. Konsekwencją modyfikacji danych dotyczących wyrobów azbestowych może być brak dostępu przez osobę fizyczną do dofinansowania na usuwanie wyrobów zawierających azbest. Podstawą do ubiegania się o środki finansowe są aktualne dane z inwentaryzacji wyrobów zawierających azbest.

Błąd polegający na nieprawidłowym wskazaniu lokalizacji występowania wyrobów zawierających azbest będzie mógł zostać usunięty m.in. wskutek dokonania weryfikacji przez wójta, burmistrza, prezydenta miasta lub marszałka województwa. Szczegółowy opis procedury zgłaszania do usunięcia błędnie wprowadzonych do systemu Bazy Azbestowej wyrobów oraz lokalizacji, w których są one położone, został przedstawiony w [Instrukcji użytkownika JST](https://www.bazaazbestowa.gov.pl/images/do-pobrania/instrukcja.pdf) w Bazie Azbestowej.

Niepożądana modyfikacja danych dotyczących wykonawców oraz jednostek szkoleniowych może wpłynąć na reputację firmy, prowadząc do utraty zaufania, a w konsekwencji partnerów biznesowych. Może to być w szczególności istotne dla wykonawców prac w kontekście posiadanego przez nich zezwolenia, np. nieprawidłowe wskazanie, że zezwolenie zostało cofnięte lub wygasło.

### Jakie są główne zagrożenia, które mogą doprowadzić do zdarzenia się ryzyka?

*Należy przedstawić zagrożenia.*

Brak prawidłowego działania Bazy Azbestowej, atak hackerski przez osobę nieupoważnioną (włamanie), błąd użytkownika Bazy Azbestowej.

### Jakie są źródła ryzyka?

*Należy źródła ryzyka.*

Incydent lub szkoda w data center (przerwa w zasilaniu, pożar, zalanie), źródła osobowe wewnętrzne - nieumyślne działanie pracownika, źródła osobowe zewnętrzne - osoba trzecia, mająca złe zamiary, haker obierający za cel naruszenie wizerunku Ministerstwa.

### Które ze zidentyfikowanych środków pozwoli zająć się ryzykiem?

*(Proszę wymienić z katalogu wcześniej zidentyfikowanych środków w zakładce „Środki istniejące lub przewidziane”.*

Dzienniki systemowe (logi), kopie zapasowe, polityka ochrony danych osobowych, kontrola dostępu logicznego, kontrola dostępu fizycznego, bezpieczeństwo sieci, ochrona przed nieosobowymi źródłami ryzyka, zabezpieczenie sprzętu (hardware), monitorowanie aktywności sieci, zabezpieczenie eksploatacji.

### Jaka jest szacowana istotność ryzyka, w zależności od potencjalnych skutków i  przewidzianych środków?

### *Skala: Pomijalne – Ograniczone – Poważne - Maksymalne*

Ograniczone.

Uzasadnienie: Zastosowane środki powodują, że prawdopodobieństwo należy uznać za ograniczone.

### Jakie jest szacowane prawdopodobieństwo ryzyka, szczególnie w odniesieniu do zagrożeń, źródeł ryzyka i przewidzianych środków?

*Skala: Pomijalne – Ograniczone – Poważne - Maksymalne*

Pomijalne.

Uzasadnienie: Zastosowane środki powodują, że prawdopodobieństwo należy uznać za pomijalne.

# Ryzyka

## Zniknięcie danych

#### Należy dokonać analizy przyczyn i konsekwencji utraty danych i oszacować jego istotność oraz prawdopodobieństwo.

### Jakie mogą być główne skutki dla osób, których dane dotyczą, jeżeli ryzyko się zdarzy?

*Należy przedstawić potencjalne skutki.*

Konsekwencją utraty danych dotyczących wyrobów azbestowych może być brak dostępu przez osobę fizyczną do dofinansowania na usuwanie wyrobów zawierających azbest. Podstawą do ubiegania się o środki finansowe są aktualne dane z inwentaryzacji wyrobów zawierających azbest.

W przypadku utraty danych dotyczących wykonawców oraz jednostek szkoleniowych może to wpłynąć na reputację firmy, prowadząc do utraty zaufania, a w konsekwencji partnerów biznesowych. Może to być w szczególności istotne dla wykonawców prac w kontekście posiadanego przez nich zezwolenia.

### Jakie są główne zagrożenia, które mogą doprowadzić do zdarzenia się ryzyka?

*Należy przedstawić zagrożenia.*

Brak prawidłowego działania Bazy Azbestowej, atak hackerski przez osobę nieupoważnioną (włamanie), błąd w zakresie nadawania uprawnień.

### Jakie są źródła ryzyka?

*Należy źródła ryzyka.*

Incydent lub szkoda w data center (przerwa w zasilaniu, pożar, zalanie), źródła osobowe wewnętrzne - nieumyślne działanie pracownika, źródła osobowe zewnętrzne - osoba trzecia, mająca złe zamiary, haker obierający za cel naruszenie wizerunku Ministerstwa.

### Które ze zidentyfikowanych środków pozwoli zająć się ryzykiem?

*(Proszę wymienić z katalogu wcześniej zidentyfikowanych środków w zakładce „Środki istniejące lub przewidziane”.*

Kopie zapasowe (przechowywane na odrębnym serwerze umiejscowionym w innej lokalizacji niż serwery produkcyjne systemu (odrębne data center), dzienniki systemowe (logi), polityka ochrony danych osobowych, kontrola dostępu logicznego, kontrola dostępu fizycznego, bezpieczeństwo sieci, nadzór, ochrona przed nieosobowymi źródłami ryzyka, zabezpieczenie sprzętu (hardware), monitorowanie aktywności sieci, bezpieczeństwo stron www, zwalczanie złośliwego oprogramowania, zabezpieczenie eksploatacji.

### Jaka jest szacowana istotność ryzyka, w zależności od potencjalnych skutków i  przewidzianych środków?

*Skala: Pomijalne – Ograniczone – Poważne - Maksymalne*

Ograniczone.

Uzasadnienie: Zastosowane środki powodują, że prawdopodobieństwo należy uznać za ograniczone.

### Jakie jest szacowane prawdopodobieństwo ryzyka, szczególnie w odniesieniu do zagrożeń, źródeł ryzyka i przewidzianych środków?

*Skala: Pomijalne – Ograniczone – Poważne - Maksymalne*

Ograniczone.

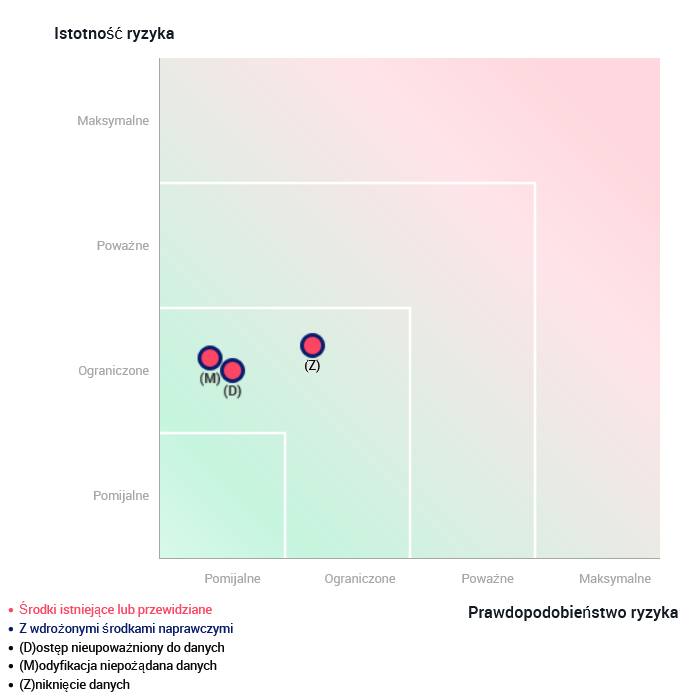
Uzasadnienie: Zastosowane środki powodują, że prawdopodobieństwo należy uznać za ograniczone.

# Obraz ryzyka

Obraz zawierający tekst, zrzut ekranu, diagram, design

Opis wygenerowany automatycznie

# Mapa ryzyka



# Sposób postępowania z ryzykami

### Ryzyka w kontekście bezpieczeństwa przetwarzania danych osobowych

### Administrator, dokonując analizy ryzyka w kontekście bezpieczeństwa przetwarzania danych osobowych, przeanalizował ryzyko naruszenia praw lub wolności osób fizycznych (Motywy 75-76 RODO). Badanie wykazało ograniczone ryzyko naruszenia praw lub wolności osób fizycznych.

### Należy zauważyć, że Baza Azbestowa była tworzona w latach 2004-2006 w celu zwiększenia tempa usuwania wyrobów zawierających azbest, jako narzędzie monitoringu realizacji Programu usuwania azbestu i wyrobów zawierających azbest stosowanych na terytorium Polski, w formie bazy danych o wyrobach i odpadach zawierających azbest. Od 2013 r. funkcjonuje jako obligatoryjny rejestr wyrobów zawierających azbest prowadzony w formie elektronicznej zgodnie z rozporządzeniem Ministra Środowiska z dnia 20 grudnia 2012 r. w sprawie sposobu prowadzenia przez marszałka województwa rejestru wyrobów zawierających azbest.

### Podstawową zmianą w stosunku do obecnie istniejących rozwiązań jest uregulowanie kwestii jednego administratora danych osobowych Bazy Azbestowej.

### W związku z powyższym administrator, mając na uwadze art. 35 ust. 1 RODO, podjął decyzję o dokonaniu oceny skutków operacji przetwarzania dla ochrony danych osobowych (DPIA). W wyniku przeprowadzonej analizy ustalono, że zagrożeniem dla praw lub wolności osób fizycznych będzie materializacja następujących ryzyk:

### - nieupoważnionego dostępu do danych,

### - niepożądanej modyfikacji danych,

### - zniknięcie/utrata danych.

### Decyzja o sposobie postępowania z ryzykami

### Administrator przeanalizował poszczególne zagrożenia, ocenił ich potencjalne skutki, wskazał źródła zagrożeń, a następnie wdrożył odpowiednie środki minimalizujące ryzyko (Obraz ryzyka).

### Administrator ocenił, że istniejące zabezpieczenia, czyli środki organizacyjne i techniczne, są wystarczające do zapewnienia odpowiedniego poziomu ochrony procesu przetwarzania danych.