Załącznik do uchwały Zarządu MZK Nr 69/VII/2021 z dnia 27.07.2021r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

w Międzygminnym Związku Komunikacyjnym w Jastrzębiu Zdroju
44-335 Jastrzębie-Zdrój, ul. Przemysłowa 1

Spis treści

I. WSTĘP

Niniejszy dokument zatytułowany **„Polityka ochrony danych osobowych"** (dalej jako **Polityka)** powstał w celu określenia standardów bezpiecznego przetwarzania danych osobowych w instytucji Administratora.

W związku z przetwarzaniem danych przez Administratora powołano niniejszą Politykę, której zadaniem jest zapewnienie przestrzegania podczas przetwarzania danych praw i wolności osób fizycznych, a w szczególności ich prawa do ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Niniejsza Polityka jest jednym z głównych środków organizacyjnych, stanowi zestaw wymogów, zasad i regulacji ochrony danych osobowych powołanych w celu zapewnienia oraz wykazania przetwarzania tych danych zgodnie z ogólnym rozporządzeniem o ochronie danych - RODO.

Polityka bezpieczeństwa zawiera procedury i ogół zasad regulujących sposobem zarządzania ochroną danych osobowych w zakresie ich przetwarzania w MZK.

Celem Polityki bezpieczeństwa jest również przyjęcie, wdrożenie i realizacja działań przy zastosowaniu odpowiednich środków technicznych i organizacyjnych, które zapewnią maksymalną ochronę procesu przetwarzania danych osobowych, chroniąc je przed udostępnieniem ich osobom nieupoważnionym, nieuprawnioną ich modyfikacją, utratą ich lub zniszczeniem.

Pracownicy są odpowiedzialni za bezpieczeństwo danych, do których mają dostęp.

Pracownicy są zobowiązani do zapoznania się z obowiązującymi przepisami dotyczącymi ochrony danych osobowych oraz do przestrzegania zasad zawartych w dokumentacji bezpieczeństwa, a także do niezwłocznego informowania Inspektora Ochrony Danych Osobowych o naruszeniu bezpieczeństwa danych osobowych.

Zarządzanie bezpieczeństwem zasobów danych osobowych stanowi proces ciągły, na który składają się takie elementy, jak: identyfikacja oraz analiza zagrożeń i ryzyka, stosowanie odpowiednich zabezpieczeń, monitorowanie wdrażania i eksploatacji zabezpieczeń, wykrywanie i reagowanie na incydenty.

Administrator deklaruje, że będzie stale doskonalić i rozwijać organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i w systemie informatycznym, tak aby skutecznie zapobiegać zagrożeniom.

W MZK przetwarza się dane osobowe jedynie niezbędne do osiągnięcia konkretnego celu przetwarzania – minimalizacja danych.

Administrator wprowadza niniejszą Politykę aby zapewnić odpowiedni stopień bezpieczeństwa w zakresie ryzyk zdefiniowanych w DPIA MZK Jastrzębie-Zdrój , a także zdolności do ciągłego zapewnienia poufności, integralności przetwarzanych danych osobowych, zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

II. DEFINICJE

Przez użyte w Polityce określenia należy rozumieć:

Polityka - oznacza niniejszą Politykę: ochrony danych osobowych.

RODO - oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE. L N 119, s. 1).

Administrator - oznacza osobę fizyczną lub prawna, organ publiczny, jednostkę: lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

W przypadku niniejszej Polityki Administratorem jest: Międzygminny Związek Komunikacyjny w Jastrzębiu Zdroju, 44-335 Jastrzębie-Zdrój, ul. Przemysłowa 1.

Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwą do zidentyfikowania osobą fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynnik6w określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Przetwarzanie - oznacza operacje: lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Szczególne kategorie danych - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Osoba - oznacza osobę fizyczną której dane dotyczą.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora; Podmiot przetwarzający jest odrębnym bytem prawnym. Może wykonywać operacje przetwarzania jedynie na udokumentowane polecenie Administratora. W obszarze ISO podmiot ten najczęściej nazywany jest - procesorem.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną

trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców.

Czynność przetwarzania - oznacza mniejszy lub większy (krótszy lub dłuższy) wycinek procesu ,,biznesowego"/ procesu przetwarzania danych realizowanego w konkretnym celu przetwarzania danych. Czynności przetwarzania danych składają się z operacji przetwarzania danych.

Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności i zachowania, lokalizacji lub przemieszczania się.

IODO lub inspektor - oznacza lnspektora Ochrony Danych Osobowych.

Zagrożenie - jest to potencjalna przyczyna niepożądanego incydentu, który *może* powodować szkody dla systemu lub organizacji. lncydenty powstają wskutek zagrożeń. Na zagrożenie i jego prawdopodobieństwo mają wpływ: okoliczności, stan prawny, stan faktyczny, działania, zaniechanie działań i wydarzenia zewnętrzne oraz wewnętrzne, które mogą ale nie muszą wywołać ryzyko wystąpienia incydentu.

lncydent bezpieczeństwa informacji - jest zdarzeniem, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie ochrony danych osobowych.

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W ISO konsekwencja, rezultat zdarzenia;

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, *że* takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Zgoda - osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Ograniczenie przetwarzania - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

Dane dotyczące zdrowia - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia ; Zgodnie z Preambułą w motywie (35) - do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby,

której dane dotyczą, ujawniające informacje o przeszłym, obecnym tub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia tej usługi opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/ 24/ UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badan laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Rejestr Czynności Przetwarzania Danych - **(RCPD)** stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się: cały system ochrony danych osobowych, czyli zasady rozliczalności. Pełni również funkcję informacyjną, w tym stanowi źródło informacji o procesach przetwarzania danych w danej organizacji dla organu nadzorczego.

Ocena Skutków Dla Ochrony Danych - jeżeli planowany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jest to sformalizowana analiza ryzyka przetwarzania danych dla sytuacji, w których to ryzyko zostało ustalone przez organizację jako wysokie.

III. OGÓLNE ZASADY OCHRONA DANYCH OSOBOWYCH

1. Zawartość polityki.

Polityka zawiera:

a) opis wymogów, zasad i regulacji ochrony danych osobowych powołanych w celu zapewnienia oraz wykazania przetwarzania danych Związku zgodnie z RODO;

b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów, procesów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

2. Odpowiedzialność.

Polityka Związku oparta jest na zasadzie odpowiedzialności:

a) odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest

Administrator {Związek} reprezentowany przez Zarząd Związku;

b) Zarząd Związku wyznacza Członka zarządu, któremu powierza nadzór nad obszarem ochrony danych osobowych w celu zapewnienia zgodności przetwarzania danych zgodnie z wymogami RODO oraz Polityką;

c) za nadzór i monitorowanie przestrzegania Polityki odpowiada powołany Inspektor Ochrony Danych (IODO);

d) za stosowanie niniejszej Polityki odpowiedzialni są:

- Związek reprezentowany przez Zarząd,
- wszyscy członkowie personelu Związku;

e) Administrator zapewnia by w przypadkach, w których zachodzi powierzenie danych, Związek korzystać będzie z usług tylko takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane im powierzono.

3. Cztery fundamenty Polityki Związku

Polityka ochrony danych Związku oparta została na czterech fundamentalnych zasadach

1) **Zasada legalności** - Związek dba by przetwarzanie danych odbywało się zgodnie z prawem dbając o ochronę prywatności.
2) **Zasada respektowania praw jednostki** - Związek umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
3) **Zasada bezpiecznego przetwarzania** - Związek zapewnia odpowiedni poziom bezpieczeństwa przetwarzania danych, analizując i monitorując ryzyko oraz zapewniając i wdrażając odpowiednie środki bezpieczeństwa.
4) **Zasada** rozliczalności - Związek dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność .

3.1. Realizacja zasady legalności

Związek przetwarza dane osobowe w poszanowaniu i realizacji następujących zasad:

a) **Legalność** - Związek przetwarza dane tylko w oparciu o podstawę: prawną, zapewniając rzetelność i przejrzystość dla i wobec osoby, której dane dotyczą.

b) **Celowość** - Związek zbiera dane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami.

c) **Adekwatność** - Związek zbiera dane adekwatnie, stosownie oraz ograniczając się: do danych niezbędnych do realizacji celów, w których są przetwarzane.

d) **Merytoryczna poprawność** - Związek gromadzi i przetwarza dane z dbałości

o ich merytoryczną poprawność i prawidłowość.

e) **Ograniczenie czasowe** - Związek zapewnia by przechowywanie danych w formie umożliwiającej identyfikacji: osoby, nie trwało przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

f) **Właściwe zabezpieczenie** - Związek dokłada wszelkiej staranności by sposób przetwarzania przez nich danych zapewniał dla nich odpowiedni poziom bezpieczeństwa, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem ("integralność i poufność").

Administrator na bieżąco prowadzi inwentaryzację czynności przetwarzania danych analizując przestrzeganie powyższych zasad legalności. Aktualny stan zasobów oraz bieżące zmiany Związek prowadzi w Rejestrze Czynności Przetwarzania Danych.

3.2. Realizacja zasady respektowania praw jednostki

3.2.1. Związek realizuje obowiązek spełnienia praw osób, których dane dotyczą poprzez:

a) dbanie o czytelność, przejrzystość, rzetelność oraz zwięzłość przekazywanych informacji w komunikacji z osobami, których dane przetwarza;

b) ułatwianie osobom w korzystaniu z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Związku oraz tablicy ogłoszeń informacji o prawach osób, sposobie skorzystania z nich, kanałach kontaktu ze Związkiem oraz ewentualnym cenniku żądań ,,dodatkowych" itp.;

c) dbanie o dotrzymywanie prawnych terminów realizacji obowiązków względem osób;

d) zapewnienie właściwej realizacji obowiązku informacyjnego przy zbieraniu danych i w innych sytuacjach.

e) stosowania procedury pozwalającej na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

3.2.2. W celu realizacji praw jednostki Związek zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Związek, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

3.2.3. Związek dokumentuje obsługę obowiązków informacyjnych, zawiadomień i incydentów osób.

Prawa osób, których dane dotyczą:

a) Prawo dostępu do informacji

b) Prawo do sprostowania danych

c) Prawo do usunięcia danych (,,prawo do bycia zapomnianym")

d) Prawo do ograniczenia przetwarzania

e) Prawo o powiadomieniu przez Administratora o sprostowaniu, usunięciu, ograniczeniu

f) Prawo do przenoszenia danych

g) Prawo do sprzeciwu

h) Prawo do niepodleganiu zautomatyzowanej decyzji

3.3. Realizacja zasady bezpiecznego przetwarzania

Zapewnienie odpowiedniego bezpieczeństwa przetwarzania danych osobowych Związek realizuje w oparciu o system ochrony danych osobowych składający się z następujących elementów:

1) **Inwentaryzacja danych.** Związek dokonuje inwentaryzacji zasobów danych osobowych w kontekście czynności przetwarzania ze szczególnym uwzględnieniem: procesów biznesowych, klas danych, zależności między zasobami, okresem przechowywania danych, identyfikacją oraz skutecznością aktualnych środków bezpieczeństwa, prawnych przesłanek przetwarzania danych, obszarów przetwarzania.

    a. pierwszą inwentaryzację Związek dokonuje poprzez przeprowadzenie ,,audytu zgodności przetwarzania danych z RODO".

    b. aktualny stan zasobów oraz bieżące zmiany Związek prowadzi w RCPD.

2) **RCPD.** Związek opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych - Rejestr. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Związku.

    a. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
    b. Związek prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

    c. Rejestr jest jednym z podstawowych narzędzi umożliwiających Związkowi rozliczanie większości obowiązków ochrony danych.

    d. W Rejestrze dla każdej czynności przetwarzania danych, której Związek uznaje za odrębną dla potrzeb Rejestru, Związek odnotowuje co najmniej:

        - nazwę czynności,
        - zakres przetwarzania (opis czynności przetwarzania-procesu biznesowego - opis etapów),

- cel przetwarzania,
- podstaw prawnych przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Związku, jeśli podstawę jest uzasadniony interes,
- kontekst oraz charakter przetwarzania,
- opis kategorii osób,
- opis kategorii danych,
- okres przechowywania,
- sposób realizacji spełnienia obowiązku informacyjnego,
- opis kategorii odbiorców danych (w tym przetwarzających),
- opis aktualnych procedur organizacyjnych,
- ogólny opis technicznych i organizacyjnych środków ochrony danych.

e. Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Związek rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, im pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

f. W ramach RCPD Związek identyfikuje oraz weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

- Utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikacji na odległość,

g. inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Związek przetwarza dane na podstawie prawnie uzasadnionego interesu Związku.

3) **Minimalizacja.** Związek posiada zasady i metody zarządzania minimalizacją *(privacy by default),* a w tym:

a. Zasady zarządzania adekwatnością - **minimalizacja zakresu:**

- Związek każdorazowo weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania;

- Związek dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

b. zasady reglamentacji i zarządzania **dostępem** do danych - **minimalizacja dostępu** (dostępu do danych):

- Związek stosuje ograniczenia dostępu do danych osobowych:

  - prawne *(zobowiązania do poufności, zakresy upoważnień),*
  - fizyczne *(strefy dostępu, zamykanie pomieszczeń),*
  - logiczne *(ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).*

- Związek nadaje dostęp do przetwarzanych danych osobowych wyłącznie tym osobom, które:
  - zostały skutecznie zapoznane z wyciągiem z podstawowych zasad bezpieczeństwa danych osobowych,
  - zobowiązały się do jego przestrzegania w drodze oświadczenia, oraz do zachowania do zachowania poufności,
  - oraz otrzymały upoważnienie, ściśle precyzujące zakres czynności, które związane są z dostępem do danych osobowych.
- Związek prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
- Związek dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról, osób, oraz zmianach podmiotów przetwarzających.
- Związek dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
- Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Związku.

c. zasady reglamentacji i zarządzania **dostępem** do danych - **minimalizacja czasu** (okres przechowywania danych):
   - Związek wdraża mechanizmy kontroli cyklu życia danych osobowych w Związku, w tym weryfikacji dalszej przydatności danych względem terminówi punktów kontrolnych wskazanych w Rejestrze.
   - Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów ~~produkcyjnych~~ Związku, jak też z akt podręcznych i głównych.

4) **Bezpieczeństwo.** Związek zapewnia odpowiedni poziom bezpieczeństwa danych, poprzez:
   a. przeprowadzanie analizy ryzyka dla czynności przetwarzania danych,
      - Związek zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
      - Związek kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka,kt6re przedstawiają.
      - Związek przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.

Związek analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniają charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

- Związek ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Związek ustala przydatność i stosuje takie środki i podejście jak:

  - pseudonimizacja,

  - szyfrowanie danych osobowych,

  - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

  - środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

b. przeprowadzanie w określonych prawem sytuacjach oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

c. dostosowywanie odpowiednich środków ochrony do ustalonego ryzyka;

d. monitorowanie właściwego działania zabezpieczeń oraz cykliczne audyty bezpieczeństwa;

e. stosuje procedury pozwalające na identyfikacje: ocen i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych - zarządca incydentami.

5) **Powierzenie przetwarzania.** Związek posiada zasady doboru przetwarzających dane na rzecz Związku, wymogów, co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

Związek zapewnia by w przypadkach, w których zachodzi powierzenie danych, korzystać będzie z usług tylko takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane im powierzono.

Związek rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też innych wymagań wynikających z Zasad powierzenia danych osobowych. Związek prowadzi rejestr umów powierzenia.

3.4. Realizacja zasady rozliczalności

Związek dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

Wszystkie działania dotyczące realizacji zasad bezpieczeństwa w Związku są dokumentowane. Szczególnymi dokumentami służącymi do potwierdzenia rozliczalności Związku są:

1) **Raport z audytu zgodności przetwarzania danych z RODO.**
2) **Analiza ryzyka dotycząca czynności przetwarzania danych.**
3) **Rejestr Czynności Przetwarzania Danych.**
4) **Ocena skutków dla ochrony danych.**
5) **Rejestr naruszeń.**
6) **Rejestr incydentów.**
7) **Rejestr wydanych upoważnień.**
8) **Rejestr umów powierzenia przetwarzania.**
9) **Rejestr obsługi zgłoszeń osób fizycznych.**

4. Osoby nie upoważnione do przetwarzania danych osobowych mogą przebywać w pomieszczeniach stanowiących obszar przetwarzania tych danych tylko w obecności pracownika posiadającego polecenie do przetwarzania danych osobowych.

Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych. W szczególności w razie nieobecności użytkownika, obowiązany on jest umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym (wylogowanie) uniemożliwiających dostęp do danych osobowych osobom niepowołanym.

Dostęp do budynków i pomieszczeń MZK, w których przetwarzane są dane osobowe podlega kontroli. Klucze do budynków i pomieszczeń posiadają tylko i wyłącznie osoby upoważnione. Budynek Zarządu przy ulicy MZK w Jastrzębiu-Zdroju jest objęty monitoringiem wizyjnym,

5. Osoby fizyczne o przetwarzaniu danych osobowych informowani są poprzez umieszczenie informacji według zakresu określonego w art. 13 rodo na stronie internetowej www.mzkjastrzebie.com w zakładce RODO. Informacja zgodnie z zakresem art. 13 rodo umieszczona jest również na tablicach ogłoszeń w biurze MZK w Jastrzębiu-Zdroju przy ulicy Przemysłowej 1. W pojazdach, które służą do przewozu osób również są wywieszone tabliczki znamionowe z realizacją obowiązku informacyjnego, gdzie jest zrealizowany taki obowiązek.

Kontrahenci MZK informowani są podpisując stosowne oświadczenie według zakresu art. 13 rodo, bądź ta informacja jest zawarta w umowie , której stroną jest kontrahent. Natomiast pracownicy są informowani potwierdzając zapoznanie się z informacją, która została im przekazana do zapoznania się zgodnie z zakresem art. 13 rodo.

6. Metody szacowania ryzyka określono w odrębnym dokumencie zatwierdzonym do stosowania w MZK jest to dokumentacja oceny skutków dla ochrony danych osobowych DPIA (Data Protection Impact Assessment).