Załącznik nr 1 do uchwały nr 19/2023
Zarządu Związku Gmin i Powiatów Subregionu Północnego
Województwa Śląskiego z siedzibą w Częstochowie
z dnia 22 listopada 2023r.

Polityka Bezpieczeństwa Informacji Stowarzyszenia „Związek Gmin i Powiatów Subregionu Północnego"

I. INFORMACJE OGÓLNE

1. Niniejszy dokument stanowi zbiór zasad i regulacji ochrony danych osobowych w Stowarzyszeniu „Związek Gmin i Powiatów Subregionu Północnego"
2. Niniejsza Polityka jest polityką ochrony danych osobowych i bezpieczeństwa informacji w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1), zwanym dalej „RODO".
3. Polityka Bezpieczeństwa Informacji, zwana dalej Polityką wprowadzana jest w celu zapewnienia zgodności działań podejmowanych przez Administratora Danych Osobowych z ustawą z dnia 10 maja 2018 o ochronie danych osobowych (Dz. U. 2019 poz. 1781), zwaną dalej „Ustawą" oraz z RODO.
4. Administratorem Danych Osobowych jest Stowarzyszenie Związek Gmin i Powiatów Subregionu Północnego Województwa Śląskiego, zwane dalej ADO.

II. DEFINICJE

1. **Administrator Danych Osobowych** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2. **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba 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 czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. **Szczególne kategorie danych** oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, dane dotyczące wyroków skazujących oraz naruszeń prawa;
4. **Integralność i poufność** oznacza przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
5. **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;
6. **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 jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
7. **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
8. **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;
9. **Poufność danych** oznacza właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
10. **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, zachowania, lokalizacji lub przemieszczania się;

11. **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;
12. **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;
13. **RODO,** rozumie się rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
14. **System informatyczny** rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
15. **Ustawa** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)
16. **Usuwanie danych** rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
17. **Uwierzytelnianie** rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
18. **Zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
19. **Strona trzecia** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, ADO, podmiot przetwarzający czy osoby, które – z upoważnienia ADO lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
20. **Zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
21. **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;

III. KATALOG INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Celem wdrożenia niniejszej dokumentacji jest ochrona interesów osób, których dane dotyczą poprzez zapewnienie należytej, adekwatnej do przewidywanych zagrożeń oraz kategorii przetwarzanych danych, ochrony posiadanych zasobów informacyjnych.
2. Wdrożenie niniejszej Polityki ma na celu zapewnienie tego by dane osobowe były przetwarzane zgodnie z zasadami RODO, tj.:
    a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
    b. rzetelnie i uczciwie (rzetelność);
    c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
    d. w konkretnych celach i nie „na zapas" (minimalizacja);
    e. nie więcej niż potrzeba (adekwatność);
    f. z dbałością o prawidłowość danych (prawidłowość)
    g. nie dłużej niż potrzeba (czasowość);
    h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

3. W celu realizacji ww. zasad, w tym w celu spełnienia wymogów RODO ADO wdraża odpowiednie środki techniczne i organizacyjne.
4. ADO uwzględnia ochronę danych i prywatności na każdym etapie tworzenia oraz istnienia technologii obejmujących ich przetwarzanie.
5. Zakres przedmiotowy stosowania niniejszej dokumentacji obejmuje wszystkie zbiory danych osobowych przetwarzane przez ADO, zarówno w formie elektronicznej, jak i papierowej oraz dane osobowe przetwarzane poza zbiorami danych.
6. Zakres podmiotowy stosowania niniejszej dokumentacji obejmuje wszystkich pracowników oraz zleceniobiorców, przy pomocy których ADO wykonuje swoje czynności, mające dostęp do danych osobowych.
7. ADO zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania. W tym celu zasady prowadzenia projektów i inwestycji przez ADO odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.
8. Osoba, której dane będą przetwarzane ma prawo do:

    a. pozyskania informacji odnośnie przetwarzania danych osobowych
    b. pozyskiwania danych osobowych (klauzule),
    c. uzyskania potwierdzenia o przetwarzaniu danych osobowych jej dotyczących oraz uzyskaniu dostępu do nich,
    d. sprostowania danych osobowych,
    e. usunięcia danych „bycia zapomnianym",
    f. ograniczenia przetwarzania danych,
    g. sprzeciwu.

Dla celów rozliczalności zaleca się dokumentowanie przez ADO zgłoszeń osób, których dane dotyczą w zakresie zgłaszanych roszczeń, o których mowa w ust. 8.

IV. PODZIAŁ OBOWIĄZKÓW OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH OSOBOWYCH

1. Niniejszy rozdział odnosi się do obowiązków:
    a. Administratora Danych Osobowych,
    b. Inspektora Ochrony Danych,
    c. Administratora Systemów Informatycznych,
    d. Innych osób upoważnionych do przetwarzania danych osobowych;

ADMINISTRATOR DANYCH OSOBOWYCH

1. Administratorem Danych Osobowych jest Stowarzyszenie Związek Gmin i Powiatów Subregionu Północnego Województwa Śląskiego.
2. Do zadań ADO należy:
    a. odpowiedzialność za przestrzeganie zasad związanych z przetwarzaniem danych osobowych, o których mowa w pkt III ust. 2 niniejszej Polityki Bezpieczeństwa Informacji,
    b. powołanie Inspektora Ochrony Danych (fakultatywnie lub obligatoryjnie)
    c. powołanie Administratora Systemów Informatycznych (fakultatywnie)
    d. zapewnienie bezpieczeństwa przetwarzanych danych osobowych,
    e. zapewnienie prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych,
    f. nadzór nad przetwarzaniem danych osobowych,
    g. zapewnienie środków technicznych i organizacyjnych niezbędnych dla zapewnienia bezpiecznego przetwarzania danych,

h. dopuszczanie do przetwarzania danych osobowych wyłącznie osób działających w oparciu o upoważnienie do przetwarzania danych osobowych,
i. prowadzenie ewidencji osób upoważnionych,
j. prowadzenie rejestru czynności przetwarzania danych osobowych,
k. należyte i terminowe udzielanie informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji zgodnie z przepisami RODO,
l. inne obowiązki przewidziane dla Inspektora Danych Osobowych (o ile nie został powołany) i/lub Administratora Systemów Informatycznych (o ile nie został powołany),
m. inne obowiązki przewidziane w niniejszej Polityce oraz w przepisach prawa krajowego i wspólnotowego,
n. spełnienie obowiązku informacyjnego na podstawie art.13 i 14 RODO stanowi **załącznik nr 6** Polityki Bezpieczeństwa Informacji.

ADO w sytuacjach przewidzianych niniejszą Polityką i przepisami ochrony danych osobowych, obowiązany jest odpowiadać na wniosek osoby, której dane dotyczą w sytuacji gdy przetwarza jej dane osobowe.

W przypadku wykazania przez osobę, której dane dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

ADO jest obowiązany poinformować bez zbędnej zwłoki innych Administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH

1. Powołanie Inspektora Ochrony Danych zwanego dalej IOD jest fakultatywne lub obligatoryjne.
2. Obligatoryjne powołanie IOD następuje w sytuacji gdy spełniona została jedna z poniższych przesłanek:
   a. przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
   b. główna działalność ADO polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
   c. główna działalność ADO polega na przetwarzaniu na dużą skalę danych wrażliwych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

3. Fakultatywne powołanie IOD następuje w pozostałych przypadkach niewskazanych w ust. 2. Każdorazowo ADO powinien ocenić, czy pomimo braku przesłanek z ust. 2, w związku z przetwarzanymi przez siebie danymi, IOD powinien być powołany.
4. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w ust.7.
5. IOD może być członkiem personelu ADO lub wykonywać zadania na podstawie umowy o świadczenie usług.
6. ADO publikuje dane kontaktowe IOD i zawiadamia o nich organ nadzorczy.
7. Do zadań IOD należy w szczególności:
   a. informowanie ADO, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub ustawy o ochronie danych osobowych i doradzanie im w tej sprawie;
   b. monitorowanie przestrzegania przepisów w sprawie ochrony danych osobowych oraz przepisów wewnętrznych dotyczących ochrony danych osobowych obowiązujących u ADO, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

d. współpraca z organem nadzorczym;
e. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z konsultacjami w sprawie oceny skutków dla ochrony danych oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

8. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
9. ADO zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
10. ADO wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
11. ADO zapewnia by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez ADO za wypełnianie swoich zadań. IOD bezpośrednio podlega najwyższemu kierownictwu ADO.
12. Osoby, których dane dotyczą, mogą kontaktować się z Inspektorem Ochrony Danych Osobowych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.
13. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
14. IOD może wykonywać inne zadania i obowiązki. ADO zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Powołanie Administratora Systemów Informatycznych jest fakultatywne.
2. Administrator Systemów Informatycznych odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych, w tym w szczególności za:
    a. nadawanie/ nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
    b. modyfikację w zakresie nadanych uprawnień do przetwarzania danych osobowych w systemach informatycznych,
    c. odbieranie uprawnień do przetwarzania danych osobowych w systemach informatycznych,
    d. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
    e. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
    f. identyfikację i analizę zagrożeń oraz ocenę ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych

Administrator Systemów Informatycznych podczas wykonywania obowiązków z zakresu ochrony danych osobowych podlega bezpośrednio ADO.

V. PRZETWARZANIE DANYCH OSOBOWYCH

1. ADO dokonuje inwentaryzacji danych:
    a. **Szczególne kategorie danych –** ADO identyfikuje przypadki, w których przetwarza lub może przetwarzać szczególne kategorie danych oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania szczególnych kategorii danych. W przypadku zidentyfikowania przypadków przetwarzania szczególnych kategorii danych, ADO postępuje zgodnie z przyjętymi zasadami w tym zakresie,

b. **Dane niezidentyfikowane** - ADO identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane,
c. **Profilowanie** – ADO identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, ADO postępuje zgodnie z przyjętymi zasadami w tym zakresie.
d. **Współadministrowanie** – ADO identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

Inwentaryzacja danych następuje w ramach Rejestru Czynności przetwarzania danych.
Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, ADO – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa przetwarzania danych osobowych odpowiadający temu ryzyku. ADO przeprowadza analizę ryzyka wg. **załącznika nr 1** Polityki Bezpieczeństwa Informacji.

VI. PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:
   a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO;
   d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;
   f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem

Przetwarzanie szczególnych kategorii danych osobowych może nastąpić w sytuacji wystąpienia przynajmniej jednej przesłanki z wymienionych w art. 9 ust. 2 RODO.

Zgoda na przetwarzanie danych osobowych, nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

Zgoda na przetwarzanie danych osobowych może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych ADO obowiązany jest usunąć wszystkie dane osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca ADO do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie. Klauzula zgody na przetwarzanie danych stanowi **załącznik nr 7** Polityki Bezpieczeństwa Informacji.

ADO dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel) ADO dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

ADO wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

Kierownik komórki organizacyjnej ADO ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes ADO, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes ADO.

VII. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. ADO obowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona. Upoważnienie może być nadane w formie papierowej lub elektronicznej.
2. Do redagowania treści upoważnień w imieniu ADO uprawniony jest IOD.
3. Upoważnienie do przetwarzania danych osobowych powinno zawierać:
    a. datę z którą zostało nadane;
    b. datę, z którą upoważnienie wygasa jeżeli jest ono nadane na czas określony;
    c. zakres upoważnienia.

Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy o pracę, bądź umowy cywilnoprawnej zawartej przez ADO z osobą, której zostało nadane, lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.

Wzór upoważnienia do przetwarzania danych stanowi **załącznik nr 8** Polityki Bezpieczeństwa Informacji pn. „Upoważnienie do przetwarzania danych osobowych" do niniejszej Polityki.

Procedura nadawania upoważnień przebiega następująco:

a. wniosek o wydanie upoważnienia składa bezpośredni przełożony osoby, której upoważnienie dotyczy
b. wniosek może być złożony w formie papierowej bądź w formie elektronicznej,
c. przed wydaniem upoważnienia, osoba, której upoważnienie jest wydawane musi zostać zapoznana z zasadami ochrony danych osobowych, w tym z obowiązującymi aktami prawnymi krajowymi i wspólnotowymi, a także z dokumentacją ochrony danych osobowych obowiązującą u ADO,
d. za zapoznanie osoby, której upoważnienie jest wydawane odpowiada bezpośredni przełożony bądź wyznaczony przez ADO Inspektor Ochrony Danych,
e. potwierdzenie zapoznania się z zasadami ochrony danych osobowych, osoba upoważniona potwierdza pisemnie w formie papierowej,(oświadczenie o zapoznaniu stanowi **załącznik nr 2** Polityki Bezpieczeństwa Informacji).

7. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, RODO oraz Polityki.
8. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia bądź rozwiązaniu umowy cywilnoprawnej.
9. Ewidencję osób upoważnionych prowadzi ADO bądź wyznaczony przez ADO Inspektor Ochrony Danych.

10. Ewidencja osób upoważnionych może być prowadzona w formie papierowej bądź elektronicznej.
11. Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi **załącznik nr 3** Polityki Bezpieczeństwa Informacji.
12. Ewidencja zawiera:

imię i nazwisko osoby upoważnionej;

a. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
b. identyfikator, jeżeli dane są przetwarzane w systemie informatycznym

ADO podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia ADO, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie ADO, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

VIII. REJESTR CZYNNOŚCI PRZETWARZANIA

1. ADO prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się wszystkie następujące informacje:
   a. imię i nazwisko lub nazwę oraz dane kontaktowe ADO oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela ADO oraz IOD;
   b. cele przetwarzania;
   c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   e. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
   f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

   Rejestr prowadzi się w formie papierowej lub elektronicznej.
   ADO udostępnia rejestr na żądanie organu nadzorczego.

Wzór rejestru czynności przetwarzania stanowi **załącznik nr 5** Polityki Bezpieczeństwa Informacji.

IX. SZKOLENIA

1. IOD lub inna osoba wyznaczona przez ADO odpowiada za zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2. Zapoznanie jest przeprowadzane przed dopuszczeniem osoby upoważnionej do czynności przetwarzania danych oraz przed nadaniem upoważnienia.
3. W celu zapewnienia stosowania przez pracowników przepisów z zakresu ochrony danych osobowych, ADO może organizować Szkolenia. Szkolenia prowadzi ADO, IOD lub osoba posiadająca wiedzę specjalistyczną z zakresu ochrony danych.
4. Przeprowadzenie szkolenia jest dokumentowane stosownymi zaświadczeniami.

X. OCENA SKUTKÓW PRZETWARZANIA

1. Jeżeli dany 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, ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Dokonując oceny skutków dla ochrony danych, ADO konsultuje się z IOD, jeżeli został on wyznaczony.
3. Ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku:
    a. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
    b. przetwarzania na dużą skalę szczególnych kategorii danych osobowych,
    c. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

    Ocena zawiera co najmniej:

    a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez ADO;
    b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
    c. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz
    d. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, ADO dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

Jeżeli ocena skutków dla ochrony danych, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby ADO nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania ADO konsultuje się z organem nadzorczym. Szczegółowa procedura opisana została w art. 36 RODO.

XI. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Szczegółowa procedura opisana została w **załączniku nr 11** Polityki Bezpieczeństwa Informacji.

XII. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. ADO przetwarza dane jedynie na obszarze do tego przeznaczonym w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.
2. Dane będą przetwarzane w siedzibie Stowarzyszenia Związku Gmin i Powiatów Subregionu Północnego Województwa Śląskiego tj. na terenie Urzędu Miasta Częstochowy.

XIII. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zachowania w tajemnicy danych osobowych, do których posiada dostęp, sposobów zabezpieczenia danych jak również wszelkich informacji, które powzięła w czasie przetwarzania danych, zarówno w sposób celowy, jak i przypadkowy. Obowiązek zachowania danych w tajemnicy obowiązuje również po ustaniu stosunku pracy bądź wygaśnięciu innych form zaangażowania personelu Stowarzyszenia Związek Gmin i Powiatów Subregionu Północnego Województwa Śląskiego tj. umów cywilnoprawnych itp.

2. Podczas przetwarzania danych trzeba zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, utratą, zniszczeniem lub ujawnieniem.
3. Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po utracie ich ważności.
4. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument trzeba zaszyfrować, a hasło przesłać, w miarę możliwości innym środkiem komunikacji elektronicznej.
6. Wszelkie dokumenty zawierające dane osobowe powinny być przechowywane w szafach lub pomieszczeniach zamykanych na klucz.
7. Osoba będąca dysponentem kluczy nie może przekazywać kluczy do pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
8. Osoba, która utraciła posiadane klucze do pomieszczeń ADO, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność ADO oraz IOD.
9. IOD oraz ADO, w zakresie swoich kompetencji, podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.
10. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej należy stosować zasadę tzw. „czystego biurka", co oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
11. Brakowanie dokumentów niearchiwalnych zawierających dane osobowe następuje po upływie okresu ich przechowywania po uznaniu przez organ, że dokumentacja utraciła wartość dowodową. Niszczenie odbywa się za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po wcześniejszym zawarciu umowy powierzenia przetwarzania danych osobowych. Fakt zniszczenia dokumentów należy odnotować w protokole.
12. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
13. Podczas korzystania z urządzeń wielofunkcyjnych typu ksero, faks, skaner należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu.
14. Przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu

1. Rozpoczęcie pracy na stacji roboczej następuje po włączeniu napięcia w listwie podtrzymującej napięcie i komputera, a następnie wprowadzeniu indywidualnego identyfikatora i znanego tylko użytkownikowi hasła.
2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w obecności użytkownika albo osoby upoważnionej do przetwarzania danych.
3. Ustawienie monitorów powinno uniemożliwiać osobom nieupoważnionym pogląd wyświetlanych treści.
4. Monitory komputerów wyposażone są we włączające się po 5 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu poprawnego hasła użytkownika.

5. W przypadku opuszczenia stanowiska pracy użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.
6. Jednostkowe dane chronione (np. osobowe) mogą być kopiowane na nośniki po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane.
7. Przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej.
8. Przetwarzając dane należy odpowiednio często wykonywać kopie robocze danych, tak by zapobiec ich utracie i umieszczać je w odpowiednich zasobach dysku sieciowego.
9. Zakończenie pracy na stacji roboczej następuje po wprowadzeniu przetwarzanych informacji w odpowiednie obszary dysku sieciowego, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w listwie przeciwprzepięciowej.
10. Przed opuszczeniem pokoju należy:
    a. zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    b. schować do zamykanych na klucz szaf wszelkie akta zawierające dane osobowe,
    c. umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
    d. zamknąć okna.
    e. zamknąć za sobą drzwi na klucz. Klucz od pokoju oddać na portierni.
11. Komputery powierzone pracownikom wynoszone poza Biuro, powinny być chronione przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas ich transportu. ADO prowadzi ewidencję komputerów przenośnych wg. **załącznika nr 4** Polityki Bezpieczeństwa Informacji.
12. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
13. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zwrócić się do administratora systemu.
14. Komputery wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację system wymusza automatycznie.

XIV. UMOWA POWIERZENIA

1. ADO może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.
2. Podmiot, któremu dane do przetwarzania powierzono, może przetwarzać dane wyłącznie w zakresie i w celu przewidzianym w umowie.
3. Rejestr umów powierzenia prowadzi IOD.
4. Wzór Rejestru umów powierzenia stanowi **załącznik nr 10** Polityki Bezpieczeństwa Informacji.
5. Umowa powierzenia powinna być zawarta w formie papierowej, w tym w formie elektronicznej.
6. Umowa powierzenia powinna zawierać następujące informacje, zgodnie z którymi podmiot przetwarzający:
    a. przetwarza dane osobowe wyłącznie na udokumentowane polecenie ADO - co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej - chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje ADO o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c. podejmuje wszelkie środki wymagane w art. 32 RODO,
d. przestrzega warunków korzystania z usług innego podmiotu przetwarzającego,
e. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga ADO poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
f. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga ADO wywiązać się z obowiązków określonych w RODO;
g. po zakończeniu świadczenia usług związanych z przetwarzaniem przekazuje cyfrowe kopie danych ADO oraz zależnie od decyzji ADO usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie danych osobowych;
h. udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym ustępie oraz umożliwia ADO lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich;
i. podmiot przetwarzający niezwłocznie informuje ADO, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.
j. udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w pkt a - i oraz umożliwia ADO lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Wzór umowy powierzenia stanowi **załącznik nr 9** Polityki Bezpieczeństwa Informacji.

XV. KONTROLA PRZESTRZEGANIA ZASAD DOTYCZĄCYCH PRZETWARZANIA DANYCH OSOBOWYCH

1. Kontrolę nad ochroną przetwarzanych danych osobowych sprawuje ADO.
2. W przypadku gdy powołano IOD lub Administratora Systemów Informatycznych, nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Stowarzyszeniu Związek Gmin i Powiatów Subregionu Północnego Województwa Śląskiego sprawuje również IOD oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
3. IOD czynności sprawdzające dokonuje w ramach audytów.

ADO ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych w trybie określonym w Polityce, o ile w umowie o powierzeniu przetwarzania danych osobowych istnieją stosowne zapisy w tym zakresie.

XVI. POSTANOWIENIA KOŃCOWE

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację ADO i obowiązuje wszystkich pracowników i współpracowników ADO oraz inne osoby przetwarzające dane osobowe przetwarzane przez ADO.
2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u ADO. Wszelkie zmiany obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u ADO.
3. Nieuzasadnione zaniechanie obowiązków wynikających z niniejszego dokumentu może stanowić podstawę do uznania, że doszło do ciężkiego naruszenia obowiązków pracowniczych lub niewykonania zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
4. W sprawach nieuregulowanych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy i RODO.

XVIII. ZAŁĄCZNIKI

1. Analiza ryzyka
2. Oświadczenie o zapoznaniu z Polityką oraz zachowaniu poufności
3. Ewidencja osób upoważnionych
4. Ewidencja komputerów przenośnych
5. Rejestr czynności przetwarzania
6. Klauzula informacyjna ogólna
7. Klauzula zgody na przetwarzanie danych
8. Upoważnienie do przetwarzania danych osobowych
9. Umowa powierzenia przetwarzania danych osobowych
10. Rejestr umów powierzenia
11. Procedura zgłaszania naruszeń

Przewodniczący Związku

Krzysztof Matyjaszczyk