UCHWAŁA NR 5/2016

Zarządu Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku z dnia 25 stycznia 2016 r.

w sprawie: przyjęcia „Polityki bezpieczeństwa danych osobowych w Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku" oraz wyznaczenia Administratora Bezpieczeństwa Informacji

Działając na podstawie § 22 ust. 2 Statutu Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku w zw. z art. 36 i art. 36a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r., 1182 ze zm.),

Zarząd Związku
uchwala, co następuje:

§ 1

Przyjmuje się „Politykę bezpieczeństwa danych osobowych w Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku", która stanowi załącznik nr 1 do uchwały.

§ 2

Wyznacza się na Administratora Bezpieczeństwa Informacji Pana Adama Wawocznego.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Zarządu
Związku Gmin i Powiatów Subregionu Zachodniego
Województwa Śląskiego z siedzibą w Rybniku

Mieczysław Kieca

Załącznik nr 1 do uchwały nr 5/2016 Zarządu Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku z dnia 25 stycznia 2016 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W ZWIĄZKU GMIN I POWIATÓW SUBREGIONU ZACHODNIEGO WOJEWÓDZTWA ŚLĄSKIEGO Z SIEDZIBĄ W RYBNIKU

SUBREGION ZACHODNI

ROZDZIAŁ I
Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa przechowywania i ochrony danych osobowych w Związku Gmin i Powiatów Subregionu Zachodniego Województwa z siedzibą w Rybniku (zwanym dalej Związkiem) jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Związek lub powierzonych mu do przetwarzania w trybie art. 31 Ustawy.
2. W Związku przetwarzane są informacje stanowiące dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2014 r. poz.1182 ze zm.).
3. Związek przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach, lub powierzone mu do przetwarzania w trybie art. 31 Ustawy w określonych celach i w określonym zakresie, jeżeli:
    a) jest to konieczne do realizacji zadań statutowych Związku,
    b) jest to niezbędne do osiągnięcia uzasadnionych celów organizacyjnych,
    c) w innym celu i zakresie, jeżeli osoba, której przetwarzane dane dotyczą, wyrazi na to pisemną zgodę.
4. Podstawą do opracowania niniejszego dokumentu i jego wdrożenia są następujące przepisy prawa:
    a) Konstytucja Rzeczypospolitej Polskiej,
    b) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2014, poz. 1182 ze zm.),
    c) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
5. Załączniki do niniejszej Polityki bezpieczeństwa danych osobowych w Związku, stanowią:
    a) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Związku – załącznik nr 1,
    b) wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe - załącznik nr 2,
    c) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych - załącznik nr 3,
    d) opis struktury zbiorów danych osobowych przetwarzanych w Związku – załącznik nr 4,
    e) sposób przepływu danych pomiędzy systemami informatycznymi - załącznik nr 5,
    f) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – załącznik nr 6,

g) ewidencja osób upoważnionych do przetwarzania danych osobowych – załącznik nr 7,
h) wzór upoważnienia do przetwarzania danych osobowych – załącznik nr 8,
i) wzór odwołania upoważnienia do przetwarzania danych osobowych – załącznik nr 8a
j) wzór upoważnienia do przetwarzania danych osobowych w ramach realizacji zadań IP RIT RPO WSL – załącznik nr 8b,
k) wzór odwołania upoważnienia do przetwarzania danych osobowych w ramach realizacji zadań IP RIT RPO WSL– załącznik nr 8c,
l) instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Związku – załącznik nr 9.

6. Przetwarzanie danych osobowych w Związku jest dopuszczalne tylko pod warunkiem przestrzegania ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2014, poz. 1182 ze zm.) i wydanych na jej podstawie przepisów wykonawczych oraz Zarządzeń Dyrektora Biura Związku w sprawie ochrony danych osobowych w Związku, a także instrukcji będących załącznikami do tego zarządzenia.

§ 2

Przez użyte w treści Regulaminu sformułowania należy rozumieć:

1. Ustawa - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2014, poz. 1182 ze zm.).
2. Dane osobowe - zestaw informacji pozwalających na jednoznaczną identyfikację konkretnej osoby w konkretnym środowisku.
3. Zbiór danych osobowych - dane osobowe zgromadzone w usystematyzowany sposób, pozwalający na łatwe dotarcie do konkretnej informacji.
4. Przetwarzanie danych - wszystkie czynności wykonywane na danych, w tym szczególnie gromadzenie, utrwalanie, modyfikacja, usuwanie, przechowywanie, przenoszenie i przekazywanie, niezależnie od formy, w jakiej wykonywane są te czynności.
5. Administrator Danych Osobowych - podmiot zajmujący się przetwarzaniem danych osobowych.
6. Administrator Bezpieczeństwa Informacji - osoba wyznaczana przez Administratora Danych Osobowych odpowiedzialna za przestrzeganie zasad ochrony danych osobowych i nadzorująca bezpieczeństwo przetwarzania danych osobowych.
7. Administrator Systemu Informatycznego - osoba wyznaczana przez Administratora Danych Osobowych odpowiedzialna za przestrzeganie zasad ochrony danych osobowych w systemie informatycznym i nadzorująca przetwarzanie danych osobowych w systemie informatycznym.
8. System informatyczny - zespół środków technicznych (urządzenia: komputerowe, drukujące, łączności, wraz z okablowaniem i oprogramowaniem), zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieć informatyczna i udostępniane przez nią zasoby.
9. Osoby zatrudnione przy przetwarzaniu danych osobowych - wszystkie osoby, w tym użytkownicy systemu informatycznego, mające z racji wykonywanych obowiązków dostęp do danych osobowych. Użytkownik systemu jest osobą upoważnioną do

przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w Związku na podstawie umowy o pracę bądź umowy cywilnoprawnej.
10. Poufność - zapewnienie dostępu do informacji wyłącznie osobom upoważnionym.
11. Integralność - spójność danych, zapewnienie, że dane nie zostaną zmienione, dodane lub usunięte w nieautoryzowany sposób.
12. Dostępność - zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy, gdy jest to uzasadnione.

ROZDZIAŁ II
Podstawy systemu bezpieczeństwa danych osobowych w Związku

§ 3

1. Administrator Danych Osobowych ma obowiązek zastosować odpowiednie środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator Danych Osobowych określa zakres przetwarzanych danych osobowych w wydawanych zarządzeniach, regulaminach lub w indywidualnych umowach z podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych.

§ 4

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez Administratora Bezpieczeństwa Informacji (Użytkownicy systemu).
2. Osoby zatrudnione w Związku przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.
3. Osoby zatrudnione w Związku przy przetwarzaniu danych osobowych przy wykorzystaniu systemów informatycznych są zobowiązane do postępowania zgodnie z Instrukcją zarządzania informatycznym systemem przetwarzania danych osobowych.

§ 5

1. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić Administratora Bezpieczeństwa Informacji o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie.
2. Rejestracji podlegają wszystkie przypadki awarii systemu, działania konserwacyjne w systemie oraz naprawy.
3. W przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą Związku, należy wymontować z niego nośniki informacji zawierające dane osobowe.
4. W przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora bezpieczeństwa informacji.

5. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych w Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w systemie informatycznym w Związku.

§ 6

W zbiorach danych administrowanych przez Związek, zabrania się przetwarzania w danych osobowych informacji ujawniających:

a) stan zdrowia,
b) pochodzenie rasowe lub etniczne,
c) poglądy polityczne,
d) przekonania religijne lub filozoficzne,
e) przynależność wyznaniową,
f) przynależność partyjną lub związkową,
g) kod genetyczny,
h) nałogi,
i) preferencje seksualne,

chyba, że wymagają tego obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła pisemną zgodę.

§ 7

1. Zabronione jest:
   a) przetwarzanie danych osobowych do których przetwarzania dany pracownik nie jest upoważniony,
   b) przetwarzanie danych osobowych, których przetwarzanie jest zabronione,
   c) przetwarzanie danych osobowych niezgodnych z celem stworzenia zbioru danych,
   d) udostępnianie lub umożliwianie dostępu do danych osobowych osobom nieupoważnionym,
   e) niezgłaszanie Administratorowi Bezpieczeństwa Informacji zbiorów danych podlegających rejestracji,
   f) niedopełnianie obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach,
   g) uniemożliwianie osobie, której dane dotyczą, korzystania z przysługujących jej praw.
2. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.
3. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencje osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
4. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

ROZDZIAŁ III
Gromadzenie danych osobowych

§ 8

Dane osobowe przetwarzane w Związku mogą być uzyskiwane:

a) bezpośrednio od osób, których te dane dotyczą,
b) z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 9

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać zmiany tych danych osobowych w sposób zapewniający anonimowość osób, których dane te dotyczą.

ROZDZIAŁ IV
Obowiązek informacyjny

§ 10

1. Pracownicy Związku, którzy zbierają i przetwarzają dane osobowe, są odpowiedzialni za poinformowanie osób, których dane przetwarzają o:
   a) adresie siedziby Związku, pod którym dane są zbierane i przetwarzane,
   b) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej,
   c) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.
2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy poinformować ponadto o:
   a) źródle danych,
   b) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 ustawy.

§ 11

Kandydaci do pracy w Związku, w procesie rekrutacji muszą podpisać pisemną zgodę na przetwarzanie ich danych osobowych lub umieścić i podpisać w składanych dokumentach odpowiednią klauzulę zezwalającą na przetwarzanie swoich danych osobowych.

ROZDZIAŁ V
Udzielanie informacji o przetwarzaniu danych osobowych

§ 12

1. Osobom, których dane przetwarza się w zbiorze danych Związku, przysługuje zgodnie z ustawą prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.

2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, musi otrzymać odpowiedź na piśmie w terminie nieprzekraczającym 30 dni od daty wpłynięcia wniosku.

§ 13

W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator Danych Osobowych jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

ROZDZIAŁ VI
Ochrona przetwarzania danych osobowych

§ 14

1. Dostęp do budynków i pomieszczeń Związku, w których przetwarzane są dane osobowe podlega monitorowaniu przez pracowników Związku.
2. Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych pomieszczeń.
3. Związek realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.

§ 15

1. Administrator Danych Osobowych Związku zobowiązany jest do wydawania, ewidencjonowania i przechowywania imiennych upoważnień do przetwarzania danych osobowych oraz cofniętych upoważnień. Upoważnienie może zostać wydane na czas określony lub do odwołania. Wydanie cofnięcia upoważnienia jest konieczne wyłącznie w przypadku uprzedniego wydania upoważnienia na czas do odwołania.
2. Administrator Danych Osobowych Związku zobowiązany jest do zbierania, ewidencjonowania i przechowywania:
   a) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność oraz stosowanych przy przetwarzaniu danych osobowych środkach bezpieczeństwa,
   b) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej o zachowaniu tajemnicy,
   c) umów zawartych w trybie art. 31 Ustawy, z osobami zatrudnionymi przy przetwarzaniu danych osobowych.
3. Brak ważnego upoważnienia, o którym mowa w punkcie 1, oraz brak podpisanych oświadczeń i porozumienia, o których mowa w punkcie 2, uniemożliwia powierzenie pracownikowi wykonywania zadań i obowiązków związanych z przetwarzaniem danych osobowych.

§ 16

1. Całkowity nadzór i kontrolę przetwarzania danych osobowych w Związku, realizuje Administrator Bezpieczeństwa Informacji. Jest on również osobą odpowiedzialną za obszar przetwarzania danych osobowych w Związku.
2. Administrator Bezpieczeństwa Informacji ma obowiązek ściśle współpracować z Administratorem Systemu Informatycznego w zakresie przetwarzania danych osobowych w systemach informatycznych.
3. Administrator Bezpieczeństwa Informacji ma obowiązek zapewnić zapoznanie się osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych oraz przeszkolić je w tym zakresie.
4. Administrator Bezpieczeństwa Informacji powołuje Administratora Systemu Informatycznego.

§ 17

W celu realizacji powierzonych zadań Administrator Bezpieczeństwa Informacji w Związku ma prawo:

a) kontrolować zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
b) wydawać polecenia w zakresie bezpieczeństwa danych osobowych,
c) informować Administratora Danych Osobowych Związku o przypadkach naruszenia bezpieczeństwa danych osobowych,
d) żądać od wszystkich pracowników wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

ROZDZIAŁ VIII
Zasady udostępniania danych osobowych

§ 18

Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 19

1. Zbiory danych udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej.
2. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
3. Wniosek jest rozpatrywany przez Administratora Bezpieczeństwa Informacji, który jednocześnie prowadzi ewidencję wniosków.
4. Decyzję w sprawie udostępnienia danych podejmuje wyłącznie Administrator Bezpieczeństwa Informacji.

§ 20

Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli:

a) spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą lub innych osób,

b) dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania Wnioskodawcy.

§ 21

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.
2. Podmiot, o którym mowa w ust. 1, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
3. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie, w jakim reguluje to zawarta umowa.
4. W przypadkach opisanych w ust. 1, 2 i 3, odpowiedzialność za ochronę przetwarzanych danych osobowych spoczywa na Administratorze Danych Osobowych, co nie wyłącza w żadnym przypadku odpowiedzialności podmiotu, z którym zawarto umowę, z tytułu przetwarzania danych niezgodnie z ustawą.
5. Przy kontroli zgodności przetwarzanych danych przez upoważniony przez Administratora Danych Osobowych podmiot, o którym mowa w ust. 1, stosuje się odpowiednio przepisy art. 14-19 ustawy.

ROZDZIAŁ IX
Postanowienia końcowe

§ 22

W sprawach nieuregulowanych niniejszym regulaminem mają zastosowanie przepisy Ustawy, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Przewodniczący Zarządu
Związku Gmin i Powiatów Subregionu Zachodniego
Województwa Śląskiego z siedzibą w Rybniku

Mieczysław Kieca

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku

Podstawa prawna

§ 1

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji (§ 3 oraz § 5) z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Postanowienia ogólne

§ 2

Ilekroć mowa w niniejszym dokumencie o Instrukcji, należy przez to rozumieć Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku.

Zakres obowiązywania niniejszej instrukcji

§ 3

Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym jak i ręcznym, zobowiązani są do zapoznania się z treścią Instrukcji i jej przestrzegania.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

§ 4

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
2. W systemie informatycznym, do którego dostęp posiadają co najmniej dwie osoby, każdy użytkownik posiada odrębny identyfikator, a dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora.
3. Przed rozpoczęciem pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. W przypadku ich wykrycia należy niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.
4. W celu rozpoczęcia pracy użytkownik wykonuje logowanie do systemu używając nadanego loginu i hasła.
5. Podczas nieobecności przy stanowisku komputerowym należy wylogować się z sytemu bądź uruchomić wygaszacz ekranu chroniony hasłem.
6. Po zakończeniu pracy w systemie należy wylogować się z sytemu i wyłączyć stację roboczą.

7. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest uprzedzone informacją do pracowników w formie wiadomości email lub osobiście przez Administratora Systemu Informatycznego na co najmniej 30 minut przed planowanym zawieszeniem.

Nadawanie uprawnień

§ 5

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.
2. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym nadaje Administrator Danych Osobowych.
3. Za rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym odpowiada Administrator Systemu Informatycznego.
4. Administrator Systemu Informatycznego nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez Administratora Danych Osobowych Związku.
5. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku zawieszenia w pełnieniu obowiązków służbowych.
6. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
7. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia również w przypadku ustania stosunku pracy.
8. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

Zabezpieczenia

§ 6

1. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
2. Hasła do systemu stacji roboczych kontrolowanych przez kontroler domeny mają długość przynajmniej 8 znaków (co najmniej litery i cyfry). Zmiana haseł następuje nie rzadziej niż co 30 dni.
3. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
4. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu "złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.
5. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza

obszarem, w którym są przetwarzane dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

6. W systemach informatycznych stosuje się fizyczne i logiczne zabezpieczenia przed nieuprawnionym dostępem. Logiczne zabezpieczenia, o których mowa w zdaniu 1 obejmują: kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemów informatycznych administratora danych.
7. Stosuje się środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Tworzenie kopii zapasowych

§ 7

1. Dane systemów kopiowane są w trybie codziennym (pn.-pt. kopie baz danych). Kopie zbiorów umieszczonych na serwerze wykonywane są automatycznie dedykowanym oprogramowaniem.
2. Dane systemów kopiowane są w trybie codziennym na przestrzeń dyskową, udostępnianą przez podmiot zewnętrzny (pn.-pt. kopie baz danych). Kopie zbiorów umieszczonych na serwerze wykonywane są automatycznie dedykowanym oprogramowaniem.
3. W przypadku likwidacji nośnika danych, na których zapisywane są kopie bezpieczeństwa niszczy się go trwale w sposób mechaniczny.
4. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza Administrator Systemu Informatycznego.

Przechowywanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

§ 8

1. Elektroniczne nośniki informacji:
   a) Danych osobowych w postaci elektronicznej (nie licząc kopii bezpieczeństwa) zapisane na dyskietkach, dyskach magnetooptycznych, dyskach twardych nie można wynosić poza siedzibę Związku.
   b) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych.
   c) Po zakończeniu pracy przez użytkowników systemu, elektroniczne nośniki informacji są przechowywane wyłącznie w zamykanych szafach biurowych.
   d) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do przetwarzania danych osobowych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie
   e) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych. W przypadku, gdy nie jest to możliwe uszkadza się je w sposób uniemożliwiający ich odczytanie. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać, itp.).

f) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.
g) Jeżeli zaistnieje sytuacja, w której urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy, przekazywane będą poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych. Szczegółowe kwestie dotyczące stosowanych środków, o których mowa w zdaniu 1 zostaną wprowadzone do Instrukcji w razie zaistnienia sytuacji, w której przetwarzane będą dane, o których mowa w art. 27 ust. 1 ustawy.

2. Wydruki:
   a) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym dostęp osobom nieuprawnionym.
   b) Pomieszczenie, w którym przechowywane są wydruki musi być zamknięte na klucz po godzinach pracy Związku.
   c) Wydruki zawierające dane osobowe w momencie przekazania do usunięcia są niszczone w sposób uniemożliwiający ich odczytanie (w specjalnej niszczarce do papieru).
   d) Poprawność przygotowania i zniszczenia nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji.

Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe

Lp.	Zbiór danych osobowych	Adres	Pomieszczenie
1.	Rejestr korespondencji	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
2.	Dane pracowników Związku	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		Biuro Rachunkowe Barbara Marek 44-210 Rybnik ul. Moniuszki 17 b	Pomieszczenia biurowe
3.	Dane osób zatrudnionych na podstawie umów cywilnoprawnych	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		IT System Sebastian Cnota ul. Brzezińska 8 a 44 – 203 Rybnik	Pomieszczenie biurowe
		Biuro Rachunkowe Barbara Marek 44-210 Rybnik ul. Moniuszki 17 b	Pomieszczenia biurowe
4.	Dane kontrahentów Związku	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		IT System Sebastian Cnota ul. Brzezińska 8 a 44 – 203 Rybnik	Pomieszczenie biurowe
		Biuro Rachunkowe Barbara Marek 44-210 Rybnik ul. Moniuszki 17 b	Pomieszczenia biurowe
5.	Rejestr wniosków o udostępnienie informacji publicznej	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		IT System Sebastian Cnota ul. Brzezińska 8 a 44 – 203 Rybnik	Pomieszczenie biurowe
6.	Dane osób funkcyjnych w organach Związku	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku	II piętro budynku - pomieszczenia Biura Związku

		ul. Białych 7 44-200 Rybnik	
		IT System Sebastian Cnota ul. Brzezińska 8 a 44 – 203 Rybnik	Pomieszczenie biurowe
7.	Dane personelu projektu, wykonawców oraz oferentów i członków komisji przetargowych zaangażowanych w projektach dofinansowanych w ramach RPO WSL	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		IT System Sebastian Cnota ul. Brzezińska 8 a 44 – 203 Rybnik	Pomieszczenie biurowe
		Urząd Marszałkowski Województwa Śląskiego w Katowicach	Pomieszczenia biurowe komórek odpowiedzialnych za realizację RPO WSL 2014 - 2020
8.	Eksperci programów operacyjnych	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		IT System Sebastian Cnota ul. Brzezińska 8 a 44 – 203 Rybnik	Pomieszczenie biurowe
		Urząd Marszałkowski Województwa Śląskiego w Katowicach	Pomieszczenia biurowe komórek odpowiedzialnych za realizację RPO WSL 2014 - 2020
		Biuro Rachunkowe Barbara Marek 44-210 Rybnik ul. Moniuszki 17 b	Pomieszczenia biurowe
9.	Osoby reprezentujące wnioskodawców i beneficjentów programów unijnych	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		IT System Sebastian Cnota ul. Brzezińska 8 a 44 – 203 Rybnik	Pomieszczenie biurowe
		Urząd Marszałkowski Województwa Śląskiego w Katowicach	Pomieszczenia biurowe komórek odpowiedzialnych za realizację RPO WSL 2014 - 2020
10.	Użytkownicy Lokalnego Systemu Informatycznego RPO WSL	Związek Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku ul. Białych 7 44-200 Rybnik	II piętro budynku - pomieszczenia Biura Związku
		IT System Sebastian Cnota ul. Brzezińska 8 a	Pomieszczenie biurowe

		44 – 203 Rybnik	
		Urząd Marszałkowski Województwa Śląskiego w Katowicach	Pomieszczenia biurowe komórek odpowiedzialnych za realizację RPO WSL 2014 - 2020

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Lp.	Zbiór danych osobowych	Rodzaj systemu/programu	
		Lokalizacja	**Nazwa programu**
1.	Rejestr korespondencji	pomieszczenia biurowe Związku	manualny – książka korespondencji
2.	Dane pracowników Związku	pomieszczenia biurowe Związku	1. manualny – teczki osobowe pracowników, 2. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		pomieszczenia biurowe Biuro Rachunkowe Barbara Marek	System informatyczny – programy: a) Kadry/Płace b) Płatnik v. 10.01.001 c) System Finansowo – Księgowy FK 2006
3.	Dane osób zatrudnionych na podstawie umów cywilnoprawnych	pomieszczenia biurowe Związku	1. manualny – skoroszyty z dokumentacjami osób zatrudnionych na podstawie umów cywilnoprawnych, 2. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet – Cobian backup 11
		pomieszczenia biurowe Biuro Rachunkowe Barbara Marek	System informatyczny – programy: a) Kadry/Płace b) Płatnik v. 10.01.001 c) System Finansowo – Księgowy FK 2006
4.	Dane kontrahentów Związku	pomieszczenia biurowe Związku	1. manualny – skoroszyty z dokumentacjami osób zatrudnionych na podstawie umów cywilnoprawnych, 2. manualny – skoroszyty z dokumentacjami udzielanych zamówień, 3. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet –

			Cobian backup 11
		pomieszczenia biurowe Biuro Rachunkowe Barbara Marek	System informatyczny – programy: a) Kadry/Płace b) Płatnik v. 10.01.001 c) System Finansowo – Księgowy FK 2006
5.	Rejestr wniosków o udostępnienie informacji publicznej	pomieszczenia biurowe Związku	1. manualny – skoroszyt zawierający rejestr wniosków o udostępnienie informacji publicznej, 2. manualny – rejestr korespondencji, 3. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet – Cobian backup 11
6.	Dane osób funkcyjnych w organach Związku	pomieszczenia biurowe Związku	1. manualny – skoroszyty z dokumentami Związku, 2. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet – Cobian backup 11
7.	Dane personelu projektu, wykonawców oraz oferentów i członków komisji przetargowych zaangażowanych w projektach dofinansowanych w ramach RPO WSL	pomieszczenia biurowe Związku	1. manualny – skoroszyty z dokumentacją dot. RPO WSL 2014 – 2020, 2. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		pomieszczenia biurowe Urzędu Marszałkowskiego	system informatyczny – LSI 2014
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet - Cobian backup 11

8.	Eksperci programów operacyjnych	pomieszczenia biurowe Związku	1. manualny – skoroszyty z dokumentacją dot. RPO WSL 2014 – 2020, 2. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		pomieszczenia biurowe Urzędu Marszałkowskiego	system informatyczny – LSI 2014
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet - Cobian backup 11
		pomieszczenia biurowe Biuro Rachunkowe Barbara Marek	System informatyczny – programy: a) Kadry/Płace b) Płatnik v. 10.01.001 c) System Finansowo – Księgowy FK 2006
9.	Osoby reprezentujące wnioskodawców i beneficjentów programów unijnych	pomieszczenia biurowe Związku	1. manualny – skoroszyty z dokumentacją dot. RPO WSL 2014 – 2020, 2. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		pomieszczenia biurowe Urzędu Marszałkowskiego	system informatyczny – LSI 2014
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet - Cobian backup 11
10.	Użytkownicy Lokalnego Systemu Informatycznego RPO WSL	pomieszczenia biurowe Związku	1. manualny – skoroszyty z dokumentacją dot. RPO WSL 2014 – 2020, 2. system informatyczny – sieć lokalna składająca się z dysku sieciowego oraz stanowisk komputerowych (programy do edycji tekstów, arkusze kalkulacyjne itp.)
		pomieszczenia biurowe Urzędu Marszałkowskiego	system informatyczny – LSI 2014
		Pomieszczenia biurowe IT System Sebastian Cnota	system informatyczny – przestrzeń dyskowa do wykonywania i przechowywania kopii bezpieczeństwa danych elektronicznych Związku wysyłanych i odbieranych za pośrednictwem sieci publicznej Internet - Cobian backup 11

Opis struktury zbiorów danych osobowych przetwarzanych w Związku.

Lp.	Zbiór danych osobowych		Zawartość poszczególnych pól informacyjnych i powiązania między nimi
1.	Rejestr korespondencji		**Zakres:** nazwiska i imiona, adres zamieszkania lub pobytu, imiona rodziców, miejsce pracy, zawód, numer telefonu, adres e – mai.
2.	Dane pracowników Związku		**Zakres:** nazwiska i imiona, adres zamieszkania lub pobytu, data urodzenia, miejsce urodzenia, seria i numer dowodu osobistego, PESEL, imiona rodziców, nazwisko panieńskie; nazwisko z poprzedniego małżeństwa; nazwisko rodowe, adres e-mail, stanowisko
3.	Dane osób zatrudnionych na podstawie umów cywilnoprawnych		**Zakres:** nazwiska i imiona, adres zamieszkania lub pobytu, data urodzenia, miejsce urodzenia, seria i numer dowodu osobistego, PESEL, imiona rodziców, nazwisko panieńskie; nazwisko z poprzedniego małżeństwa; nazwisko rodowe, adres e-mail
4.	Dane kontrahentów Związku		**Zakres:** nazwiska i imiona, adres zamieszkania lub pobytu, data urodzenia, miejsce urodzenia, seria i numer dowodu osobistego, PESEL, imiona rodziców, nazwisko panieńskie; nazwisko z poprzedniego małżeństwa; nazwisko rodowe, adres e-mail
5.	Rejestr wniosków o udostępnienie informacji publicznej		**Zakres:** nazwiska i imiona, adres zamieszkania lub pobytu, imiona rodziców, miejsce pracy, zawód, numer telefonu, adres e- mail
6.	Dane osób funkcyjnych w organach Związku		**Zakres:** nazwiska i imiona, adres zamieszkania lub pobytu, data urodzenia, miejsce urodzenia, seria i numer dowodu osobistego, PESEL, imiona rodziców, nazwisko panieńskie; nazwisko z poprzedniego małżeństwa; nazwisko rodowe, adres e-mail, stanowisko
7.	Dane personelu projektu, wykonawców oraz oferentów i członków komisji przetargowych zaangażowanych w projektach dofinansowanych w ramach RPO WSL	7a. Personel projektu zaangażowany w projektach dofinansowanych w ramach RPO WSL: kraj, stanowisko, forma zaangażowania, data zaangażowania, okres zaangażowania w projekcie, wymiar czasu pracy, planowany czas pracy	**Zakres:** imiona i nazwiska, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, numer telefonu

		7b. Wykonawcy realizujący umowy o zamówienia publiczne, których dane będą przetwarzane w związku z badaniem kwalifikowalności środków w projekcie (w tym osoby prowadzące działalność gospodarczą) oraz oferenci zaangażowani w projektach dofinansowanych w ramach RPO WSL: nazwa wykonawcy, kraj, REGON wykonawcy	
8.	Eksperci programów operacyjnych		**Zakres:** nazwiska i imiona, adres e - mail, numer telefonu
9.	Osoby reprezentujące wnioskodawców i beneficjentów programów unijnych		**Zakres:** nazwiska i imiona, miejsce pracy, stanowisko, numer telefonu, adres email
10.	Użytkownicy Lokalnego Systemu Informatycznego RPO WSL		**Zakres:** nazwiska i imiona, identyfikator użytkownika (login), adres e-mail, numer telefonu, rodzaj użytkownika, instytucja.

Sposób przepływu danych pomiędzy systemami informatycznymi

Lp.	Zbiór danych osobowych	Rodzaj systemu/programu	Sposób współpracy
1.	Rejestr korespondencji	manualny	brak przepływu danych
2.	Dane pracowników Związku	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
3.	Dane osób zatrudnionych na podstawie umów cywilnoprawnych	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
4.	Dane kontrahentów Związku	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
5.	Rejestr wniosków o udostępnienie informacji publicznej	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
6.	Dane osób funkcyjnych w organach Związku	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
7.	Dane personelu projektu, wykonawców oraz oferentów i członków komisji przetargowych zaangażowanych w projektach dofinansowanych w ramach RPO WSL	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
8.	Eksperci programów operacyjnych	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
9.	Osoby reprezentujące wnioskodawców i beneficjentów programów unijnych	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,
10.	Użytkownicy Lokalnego Systemu Informatycznego RPO WSL	1. manualny, 2. system informatyczny	przepływ dwukierunkowy, realizowany w sposób półautomatyczny,

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Lp.	Zbiór danych osobowych	Środki
1.	Rejestr korespondencji	**I. Środki ochrony fizycznej danych:** a) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie, b) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych, c) zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie, d) kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej szafie, e) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów, f) pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczone przed dostępem osób nieuprawnionych w czasie nieobecności w nim osób upoważnionych do przetwarzania danych osobowych, g) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy. h) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). i) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez
2.	Dane pracowników Związku	
3.	Dane osób zatrudnionych na podstawie umów cywilnoprawnych	
4.	Dane kontrahentów Związku	
5.	Rejestr wniosków o udostępnienie informacji publicznej	
6.	Dane osób funkcyjnych w organach Związku	
7.	Dane personelu projektu, wykonawców oraz oferentów i członków komisji przetargowych zaangażowanych w projektach dofinansowanych w ramach RPO WSL	
8.	Eksperci programów operacyjnych	
9.	Osoby reprezentujące wnioskodawców i beneficjentów programów unijnych	
10.	Użytkownicy Lokalnego Systemu Informatycznego RPO WSL	

		system monitoringu z zastosowaniem kamer przemysłowych. j) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony. k) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy. **II. Środki sprzętowe, informatyczne i telekomunikacyjne:** a) sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby beneficjenta. b) oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie. c) dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. d) zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe. e) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego. f) zastosowano kryptograficzne środki ochrony danych osobowych. g) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika. h) zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. i) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł. j) zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych. k) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.

		III. Środki organizacyjne: a) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. b) osoby zatrudnione przy przetwarzaniu danych osobowych przeszkolono w zakresie zabezpieczeń systemu informatycznego, c) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy. d) monitory komputerów, na których są przetwarzane dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane, e) przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą administratora danych osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych

Załącznik nr 7 do Polityki bezpieczeństwa ochrony danych osobowych
w Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Zbiór danych osobowych	Rodzaj systemu	Nr upoważnienia /cofnięcia upoważnienia	Data nadania / odebrania uprawnień	Podpis Administratora	Uwagi

Upoważnienie do przetwarzania danych osobowych nadane przez Administratora Bezpieczeństwa Informacji

Rybnik, dnia ……

Pan/Pani…… …….
zatrudniony/a w Związku Gmin i Powiatów
Subregionu Zachodniego Województwa Śląskiego
z siedzibą w Rybniku na stanowisku
……..

UPOWAŻNIENIE nr ….

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

u p o w a ż n i a m

Pana/Panią do przetwarzania danych osobowych w następujących zbiorach:

- …….
- …….

Zgodnie z art. 39 ust. 2 ustawy o ochronie danych osobowych, ma Pan/Pani obowiązek zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia.

Niniejsze upoważnienie:

1) zostało wydane na czas ……
2) może być w każdym czasie cofnięte,
3) wygasa z dniem rozwiązania stosunku pracy z upoważnionym pracownikiem.

……..
(podpis ABI)

Ja, niżej podpisany/a ……..oświadczam, iż zostałe/am zaznajomiony/a z przepisami dotyczącymi ochrony danych osobowych oraz pouczony/a o obowiązku zachowania w tajemnicy informacji uzyskanych w trakcie dokonywania operacji związanych z przetwarzaniem danych osobowych, również po ustaniu zatrudnienia.

……
(data i podpis pracownika)

Rybnik, dnia ……

Pan/Pani…… …….
zatrudniony/a w Związku Gmin i Powiatów
Subregionu Zachodniego Województwa Śląskiego
z siedzibą w Rybniku na stanowisku
……..

ODWOŁANIE UPOWAŻNIENIA nr _____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Odwołuję upoważnienie Pani/Pana* …….. nr ……. do przetwarzania danych osobowych wydane w dniu …… na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r. poz. 1182, ze zm.).

…..……
Data, czytelny podpis osoby upoważnionej
do wydawania i odwoływania upoważnień.

UPOWAŻNIENIE Nr____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem …….. r., na podstawie:

- art. 37, w związku z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r. poz. 1182, z późn. zm.),
- Porozumienia nr 11/RR/2015, z dn. 13 marca 2015 r. w sprawie powierzenia zadań z zakresu realizacji instrumentu Regionalne Inwestycje Terytorialne w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014–2020 z późn. zm.,

upoważniam Panią/Pana*: ……do przetwarzania danych osobowych w zbiorze/zbiorach:
1.……
2.……

Upoważnienie wygasa z chwilą ustania Pana/Pani* zatrudnienia w …….…… lub z chwilą jego odwołania.

_____
Czytelny podpis, osoby upoważnionej
do wydawania i odwoływania upoważnień.

OŚWIADCZENIE OSOBY UPOWAŻNIANEJ

Oświadczam, że zapoznałem/am* się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. poz. 1182, z późn. zm.), a także z obowiązującymi w Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku Polityką bezpieczeństwa ochrony danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r. poz. 1182 z późn. zm.), również po ustaniu zatrudnienia, odwołaniu upoważnienia, upływie jego ważności.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie zatrudnienia w Związku Gmin i Powiatów Subregionu Zachodniego Województwa Śląskiego z siedzibą w Rybniku, jak też po jego ustaniu.

Mam świadomość odpowiedzialności karnej wynikającej z art. 51-52 ustawy o ochronie danych osobowych, a także art. 266 Kodeksu karnego.

…..……

Czytelny podpis osoby składającej oświadczenie

Upoważnienie otrzymałem/am

……

(miejscowość, data, podpis)

*niepotrzebne skreślić

ODWOŁANIE UPOWAŻNIENIA nr _____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Odwołuję upoważnienie Pani/Pana* …….. nr ……. do przetwarzania danych osobowych wydane w dniu …… na podstawie:

- art. 37, w związku z art. 31 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r. poz. 1182, z późn. zm.),
- Porozumienia nr 11/RR/2015, z dn. 13 marca 2015 r. w sprawie powierzenia zadań z zakresu realizacji instrumentu Regionalne Inwestycje Terytorialne w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014–2020 z późn. zm.,

…..……..……

Data, czytelny podpis osoby upoważnionej
do wydawania i odwoływania upoważnień.

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Związku.

I. Postępowanie w przypadku naruszenia ochrony danych osobowych:

1. W przypadku stwierdzenia naruszenia:
   a) zabezpieczenia systemu informatycznego,
   b) stanu urządzeń,
   c) zawartości zbioru danych osobowych,
   d) wynikającego z ujawnienia metody pracy lub sposobu działania programu,
   e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. pożar itp.)
   g) każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest obowiązany niezwłocznie powiadomić o tym fakcie administratora systemu i administratora bezpieczeństwa informacji.

2. Pracownicy, którzy stwierdzili naruszenie ochrony danych osobowych, w oczekiwaniu na podjęcie czynności przez administratora bezpieczeństwa informacji muszą:
   a) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   b) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   c) wstrzymać bieżącą pracę w celu zabezpieczenia miejsca zdarzenia,
   d) zaniechać, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   e) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   f) udokumentować wstępnie zaistniałe naruszenie,
   g) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji lub osoby upoważnionej.

3. Administrator bezpieczeństwa informacji:
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze wnioski z przeprowadzonych wcześniej symulacji zagrożeń oraz politykę bezpieczeństwa w tym zakresie,
   b) żąda dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.

4. Administrator bezpieczeństwa informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien w szczególności zawierać:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia i powiadomienia,
   c) określenie rodzaju naruszenia i okoliczności towarzyszących,
   d) opis podjętego działania i metody postępowania,
   e) wstępną ocenę przyczyn wystąpienia naruszenia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

5. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu administrator bezpieczeństwa informacji zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. Zaistniałe naruszenie powinno stać się przedmiotem szczegółowej, zespołowej analizy .

7. Analiza, o której mowa w pkt. 7, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

II. Postanowienia końcowe

8. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszej Instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

9. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej procedury mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez pracownika, który wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomił o tym administratora bezpieczeństwa informacji.