POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Wielkopolskie Samorządowe Centrum Kształcenia Zawodowego i Ustawicznego w Gnieźnie z siedzibą przy ul. Mieszka I 27, 62-200 Gniezno

Data wprowadzenia:	17-10-2018 r.
Opracował:	Jacek Andrzejewski- inspektor ochrony danych
Zatwierdził:	Elżbieta Kabzińska- Dyrektor

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Spis treści

1. Cel, zakres zastosowania i definicje

1.1. Cel Polityki

Celem opracowania i wprowadzenia niniejszej Polityki jest opisanie zastosowanych wewnątrz Wielkopolskiego Samorządowego Centrum Kształcenia Zawodowego i Ustawicznego w Gnieźnie (dalej: WSCKZiU) środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednich do ryzyka naruszenia praw i wolności w związku z przetwarzaniem danych osobowych. Polityka ma umożliwić należyte wywiązywanie się z obowiązków administratora danych – WSCKZiU. Polityka została opracowana stosownie do przepisów Rozporządzenia 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 (dalej: RODO). Niniejszy dokument będzie wdrożony poprzez jego opublikowanie oraz zapoznawania z nim osób upoważnionych do przetwarzania danych osobowych, a także innych osób mających dostęp do danych osobowych przetwarzanych przez WSCKZiU.

1.2. Zakres zastosowania

1. Polityka obejmuje swym zakresem wszystkie dane osobowe przetwarzane przez WSCKZiU.
2. Zapisy i wymagania niniejszej Polityki mogą być wyłączone tylko w przypadku, gdy:
   1) obowiązujące przepisy prawa polskiego lub Unii Europejskiej przewidują takie wyłączenie,
   2) WSCKZiU przetwarza dane osobowe na podstawie Umowy powierzenia przetwarzania danych osobowych[1] jako podmiot przetwarzający (tzw. „Procesor") a administrator danych osobowych, który zlecił WSCKZiU proces przetwarzania danych, doręczył WSCKZiU własną Politykę bezpieczeństwa danych osobowych.

1.3. Definicje

W Polityce użyto określeń o poniższym znaczeniu:

1) Administrator lub AD	Wielkopolskie Samorządowe Centrum Kształcenia Zawodowego i Ustawicznego w Gnieźnie- w odniesieniu do danych osobowych, co do których decyduje o celach i sposobach przetwarzania;

[1]Powierzenie przetwarzania w rozumieniu art. 28 RODO

2) dane osobowe	oznaczają wszelkie 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) dane osobowe zwykłe	wszystkie dane osobowe niewchodzące w zakres tzw. danych osobowych wrażliwych czyli na gruncie art. 9 ust. 1 RODO- szczególnych kategorii danych;
4) szczególne kategorie danych	dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby oraz dane wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;
5) Prezes urzędu	Prezes Urzędu Ochrony Danych Osobowych;
6) hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
7) identyfikator użytkownika	ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8) integralność danych	właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) 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;
10) 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;
11) osoba upoważniona	osoba posiadające upoważnienie do przetwarzania danych osobowych;
12) podmiot danych (lub właściciel danych)	każda osoba fizyczna, której dane osobowe są przetwarzane przez WSCKZiU lub na zlecenie WSCKZiU w związku z prowadzoną przez nią działalnością;
13) poufność danych	właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
14) Pracownik	osoba, posiadająca dostęp do danych osobowych, świadcząca pracę na rzecz WSCKZiU na podstawie stosunku pracy;
15) strona trzecia	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
16) Procesor	osoba prawna, osoba fizyczna, jednostka organizacyjna nieposiadająca osobowości prawnej lub inny podmiot, który nie decyduje o celach i sposobach przetwarzania danych osobowych, któremu WSCKZIU: • powierzyło do przetwarzania dane osobowe oraz • zawarło Umowę powierzenia przetwarzania danych osobowych w rozumieniu art. 28 RODO lub przetwarzanie odbywa się na podstawie innego wiążącego instrumentu prawnego w rozumieniu art. 28 RODO;
17) przetwarzanie danych osobowych	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;
18) Polityka	niniejszy dokument - Polityka bezpieczeństwa danych osobowych w WSCKZiU;
19) rozliczalność	właściwość umożliwiająca wykazanie zgodności WSCKZiU z przepisami RODO;
20) RODO lub Ogólne rozporządzenie o ochronie danych	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;
21) sieć telekomunikacyjna	systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju (art. 2 pkt 35) ustawy 16 lipca 2004 roku Prawo telekomunikacyjne t.j. Dz. U. z 2014 nr 0 poz. 243 ze zm.);
22) 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;
23) publiczna sieć telekomunikacyjna	sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych (art. 2 pkt 29) ustawy 16 lipca 2004 roku Prawo telekomunikacyjne t.j. Dz. U. z 2014 nr 0 poz. 243 ze zm.);
24) Rejestr czynności przetwarzania	prowadzony przez inspektora ochrony danych rejestr zawierający minimum następujące dane: a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych; b) cele przetwarzania; c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych; 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, 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, o których mowa w art. 32 ust. 1;
25) skarga	jakiekolwiek pismo (w postaci papierowej lub elektronicznej) przekazane przez podmiot danych (właściciela danych) lub Prezesa Urzędu z treści którego wynika niezadowolenie lub żądanie wyjaśnień / informacji dotyczących przetwarzania danych osobowych przez WSCKZiU;
26) system informatyczny (lub system IT)	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
27) teletransmisja	przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
28) Ustawa	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
29) upoważnienie	jedno z poniższych: - pisemne upoważnienie wydane na podstawie art. 29 RODO do przetwarzania danych osobowych nadane Pracownikowi, Współpracownikowi lub pracownikowi Procesora przez AD, lub innego pełnomocnika WSCKZIU umocowanego do nadawania upoważnień do przetwarzania danych osobowych, - Umowa powierzenia przetwarzania danych osobowych zawarta na piśmie lub inny wiążący instrument prawny w rozumieniu art. 28 RODO;
30) usuwanie danych	zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na

	ustalenie tożsamości osoby, której dane dotyczą;
31) uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
32) użytkownik systemu IT	użytkownik systemu informatycznego, któremu nadano prawa dostępu do dowolnego systemu informatycznego należącego do WSCKZIU;
33) Współpracownik	osoba, posiadająca dostęp do danych osobowych wykonująca osobiście i bezpośrednio zadania / usługi na rzecz WSCKZIU na innej podstawie prawnej niż stosunek pracy, bez względu na nazwę lub rodzaj łączącej strony umowy;
34) zabezpieczenie danych	wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
35) zgoda osoby, której dane dotyczą	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;

2. Obowiązki WSCKZiU jako administratora danych

2.1. Obowiązek spełnienia podstaw prawnych dla przetwarzania danych osobowych

Każdy Pracownik lub Współpracownik:

1) przed podjęciem decyzji o utworzeniu celu przetwarzania lub

2) poszerzenia zakresu zbieranych danych osobowych do aktualnego celu przetwarzania określonego w Rejestrze czynności przetwarzania (RCP)

jest zobowiązany do wskazania podstawy prawnej (z RODO) legalizującej przetwarzania takich danych. W przypadku jakichkolwiek wątpliwości należy skonsultować takie zmiany z inspektorem ochrony danych Jackiem Andrzejewskim, e-mail: iod@wsckziu.gniezno.pl, tel. 601 140 404.

2.2. Obowiązek informacyjny w stosunku do podmiotu danych (art. 13 i art. 14)

1) Każdy Pracownik lub Współpracownik, który zbiera (pozyskuje) dane osobowe, w momencie ich zbierania bezpośrednio od właściciela danych, jest on zobowiązany poinformować właściciela danych (np. poprzez przedstawienie odpowiedniego klauzuli) zgodnie z ***Polityką informacyjną w zakresie wykonywania obowiązku informacyjnego z art. 13 i art. 14 RODO.***

2) W przypadku zbierania danych od osób trzecich, właściciela danych należy poinformować niezwłocznie po utrwaleniu danych o okolicznościach przetwarzania zgodnie z ***Polityką informacyjną w zakresie wykonywania obowiązku informacyjnego z art. 13 i art. 14 RODO.***

3) W przypadku korzystania z systemów informatycznych, które automatycznie zbierają dane osobowe, należy zapewnić, aby system ten udzielał informacji, o których mowa w punktach powyżej 2.2. 1) lub 2.2. 2).

4) W przypadku korzystania z podmiotów trzecich (np. agencje marketingowe, agencje rekrutacyjne prowadzące nabór na wolne stanowiska pracy) należy zapewnić w umowie z takim podmiotem, aby w trakcie zbierania danych osobowych, podmiot ten wykonywał obowiązek informacyjny w imieniu WSCKZiU zgodnie z punktem 2.2. 1) lub 2.2. 2).

2.3. Obowiązek przestrzegania zasad przetwarzania (art. 5)

W trakcie procesów przetwarzania danych osobowych należy dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności przestrzegania zasad określonych w punkcie 5. niniejszej Polityki. Obowiązek ten dotyczy zarówno Pracowników i Współpracowników WSCKZiU jak i podmiotów, które w imieniu WSCKZiU przetwarzają dane osobowe.

2.4. Obowiązek zawarcia umowy powierzenia przetwarzania danych osobowych (art. 28)

Jeśli WSCKZiU podejmie decyzję o korzystaniu z usług podmiotu trzeciego, a w ramach świadczenia tych usług podmiot ten będzie przetwarzał dane osobowe na zlecenie lub w imieniu WSCKZiU, to należy zapewnić, aby przed przekazaniem danych temu podmiotowi, została zawarta *„Umowa powierzenia przetwarzania danych osobowych”* zgodnie z zasadami określonymi w punkcie 6. niniejszej Polityki. Jeśli z jakichkolwiek względów przetwarzanie nastąpiło bez zawarcia umowy powierzenia wówczas należy niezwłocznie zadbać o podpisanie ww. dokumentu.

2.5. Obowiązek realizacji żądań osoby, której dane dotyczą

1) Jeśli właściciel danych zgłosi się z ustnym lub pisemnym wnioskiem / prośbą o dostęp / kopię danych / przeniesienie danych / usunięcie jego danych / sprostowanie / ograniczenie / zaktualizowanie (niezależnie od formy zgłoszenia papierowo lub elektronicznie) należy niezwłocznie, maksymalnie w ciągu 30 dni zrealizować taki wniosek, jeśli jest zasadny. Przedmiotowy wniosek zostać zrealizowany zgodnie z ***„Procedurą realizacji prawa dostępu do danych osób, których dane dotyczą”***

2) Pracownik lub Współpracownik wskazany do realizacji takiego wniosku ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22 RODO. Jeśli

WSCKZiU nie możne wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. Administrator odmawia podjęcia działań na żądanie osoby, której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 15–22 RODO.

2.6. Obowiązek zabezpieczenia danych

1) Każdy Pracownik i Współpracownik jest zobowiązany stosować zabezpieczenia:
   - organizacyjne (np. polityki, regulaminu, procedury) obowiązujące w WSCKZiU niezależnie do tego jakim dokumentem wewnętrznym zostały one opisane oraz
   - techniczne (np. stosowanie haseł dostępowych, szyfrowany PENDRIVE, dysk). Obchodzenie zabezpieczeń określonych w dokumentach wewnętrznych lub wdrożonych przez dostawcę IT może stanowić naruszenie ochrony danych osobowych.
2) Obowiązek zabezpieczenia danych dotyczy również Procesorów. Szczegółowe wymagania odnośnie zabezpieczania danych osobowych przez procesora powinny być określone w „*Umowie powierzenia przetwarzania danych osobowych*"

2.7. Obowiązek zgłoszenia nowego celu przetwarzania danych osobowych

1) Jeśli Pracownik lub Współpracownik podejmie decyzję o rozpoczęciu zbierania danych osobowych w nowym celu, jest zobowiązany przed przystąpieniem zbierania poinformować o tym fakcie inspektora ochrony danych na adres: iod@wsckziu.gniezno.pl lub telefonicznie na nr tel. 601 140 404.
2) Na podstawie informacji od Pracownika lub Współpracownika inspektor ochrony danych podejmuje decyzję czy dany cel podlega obowiązkowi zarejestrowania go Rejestrze czynności przetwarzania.
3) Pracownicy i Współpracownicy są zobowiązani zgłosić do inspektora ochrony danych na adres iod@wsckziu.gniezno.pl wszelkie zmiany dotyczące czynności przetwarzania opisanych w Rejestrze czynności przetwarzania.

2.8. Obowiązki przy przekazywaniu do państw trzecich

1) Europejski Obszar Gospodarczy (EOG) (ang. EEA – European Economic Area) to państwa UE oraz Islandia, Norwegia, Liechtenstein.

2) Przez podjęciem decyzji o przekazaniu danych do państwa trzeciego należy to skonsultować z inspektorem ochrony danych.

3) Przed przekazaniem danych do państwa trzeciego należy spełnić wymagania określone w Rozdziale V Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych RODO.

3. Obowiązki i odpowiedzialność

3.1. Obowiązki i odpowiedzialność wszystkich Pracowników i Współpracowników

Każdy Pracownik i Współpracownik, niezależnie od stanowiska czy zadań jest zobowiązany do i odpowiada za:

1) zachowanie w poufności danych osobowych oraz sposobu ich zabezpieczeń,
2) zapoznanie i stosowanie się do zapisów niniejszej Polityki oraz dokumentów wewnętrznych wydanych na podstawie niniejszej Polityki,
3) pisemne potwierdzenie zapoznania się z przepisami o ochronie danych osobowych i niniejszą Polityką,
4) przestrzeganie przepisów o ochronie danych osobowych w szczególności Ustawy,
5) nieudostępnianie (**bez wyjątku nikomu**) swoich haseł do systemów IT,
6) nieudostępnianie lub nieumożliwianie dostępu do danych osobowych osobom nieupoważnionym,
7) zgłaszanie każdego zauważonego incydentu / podejrzenia naruszenia ochrony danych osobowych lub niniejszej Polityki na adres inspektora ochrony danych: iod@wsckziu.gniezno.pl.

3.2. Obowiązki i odpowiedzialność kierowników komórek organizacyjnych

Każdy kierownik komórki organizacyjnej, niezależnie od stanowiska dodatkowo jest zobowiązany do i odpowiada za:

1) nadzorowanie podległych pracowników czy stosują zasady opisane w niniejszej Polityce,
2) zgłaszanie do inspektora ochrony danych na adres iod@wsckziu.gniezno.pl lub na nr telefonu: 601 140 404 potrzeb informacyjnych / szkoleniowych w zakresie przepisów o ochronie danych osobowych,

3) zgłaszanie do inspektora ochrony danych na adres iod@wsckziu.gniezno.pl lub na nr telefonu: 601 140 404 wszelkich zmian dotyczących celów przetwarzania danych osobowych **przed ich wprowadzeniem**,
4) nadzorowanie przypisanych celów przetwarzania danych osobowych czy zakres przetwarzania zgodnie z Rejestrem czynności przetwarzania,
5) konsultowanie z inspektorem ochrony danych planowych nowych rozwiązań informatycznych, które wiążą się z transferem danych osobowych do podmiotu trzeciego,
6) zapewnienie zawarcia umowy powierzenia przetwarzania przez WSCKZiU z każdym podmiotem, z którym WSCKZiU zamierza zawrzeć umowę a w wyniku realizacji tej umowy może dojść do powierzenia przetwarzania danych osobowych (po uprzednim przygotowaniu umowy przez inspektora ochrony danych).

3.3. Obowiązki i odpowiedzialność pracownika oraz dostawców IT

Każdy pracownik odpowiadający za obsługę IT oraz pracownik dostawcy IT przydzielony do współpracy z WSCKZiU jest zobowiązany do i odpowiada za:

1) nadzorowanie czy wdrożone i utrzymywane zabezpieczenia (fizyczne, logiczne, systemowe) są skutecznie,
2) nadzorowanie czy wdrożone ograniczenia dostępów do obszarów przetwarzania danych są skuteczne,
3) uwzględniania przepisów RODO oraz Polityki w trakcie projektowania i wdrażania nowych rozwiązań dotyczących bezpieczeństwa informatycznego lub fizycznego,
4) na wniosek inspektora ochrony danych, sporządzanie opinii i informacji dotyczących zabezpieczeń stosowanych w WSCKZIU.

4. Zasady postępowania w przypadku skarg/wniosków na przetwarzanie danych osobowych

4.1. Skargi / wnioski wnoszone przez właściciela danych

1) W przypadku pisemnej skargi / wniosku (niezależnie od formy doręczenia czy zatytułowania) przesłanej przez właściciela danych do WSCKZiU należy rozpatrzyć niezwłocznie, nie dłużej niż w terminie nie przekraczającym 30 dni od daty wpłynięcia.

2) Odpowiedź na skargę / wniosek należy udzielić na piśmie (z pocztowym potwierdzeniem odbioru) jeśli wnoszący podał adres do doręczeń natomiast w przypadku braku takiego adresu tą samą drogą, którą skarga / wniosek zostało złożone, chyba, że wnioskujący poprosił o inną formę. W przypadku odpowiedzi za pomocą poczty elektronicznej kopię odpowiedzi należy przesłać na adres iod@wsckziu.gniezno.pl.
3) Jeśli właściciel danych zgłosi się z wnioskiem, prośbą o zmianę lub aktualizację danych osobowych, należy uczynić to niezwłocznie po uzyskaniu takiego wniosku.
4) Jeśli właściciel danych zgłosi się z wnioskiem, prośbą o usunięcie lub zaprzestania przetwarzania jego danych, a dane te były zbierane tylko **na podstawie zgody** tej osoby, należy usunąć niezwłocznie jego dane osobowe lub zaprzestać przetwarzania do celów na jakie wyraził wcześniej zgodę.
5) Dane osobowe przetwarzane na podstawie zawartej umowy, po odwołaniu wszystkich zgód właściciela danych, mogą być nadal w innych celach (np. wykonanie umowy, podatkowe), jeśli takowe wynikają z Rejestru czynności przetwarzania.
6) Jeśli właściciel danych zgłosi się z wnioskiem o dostęp do jego danych osobowych lub uzyskanie kopii danych to na taki wniosek należy odpowiedzieć niezwłocznie, nie przekraczając 30 dni.
7) Właściciel danych może skorzystać z prawa do kopii danych nie częściej niż raz na 6 miesięcy. Jeśli jednak złoży tak wniosek wcześniej niż przed upływem 6 miesięcy, WSCKZiU może naliczyć rozsądną opłatę administracyjna związaną z przygotowaniem takiej kopii danych.
8) W przypadku wątpliwości, Pracownik może skonsultować postępowanie z inspektorem ochrony danych wysyłając wiadomość na adres iod@wsckziu.gniezno.pl bądź konsultując telefonicznie pod nr telefonu 601 104 404.
9) Sposób postępowania reguluje także ***Procedura realizacji prawa dostępu do danych osób, których dane dotyczą.***

4.2. Skargi przekazywane przez Prezesa urzędu

1) W przypadku skargi złożonej przez właściciela danych do Prezesa Urzędu, które organ przekazał do WSCKZiU, należy niezwłocznie przekazać do inspektora ochrony danych na adres iod@wsckziu.gniezno.pl oraz Dyrektorowi szkoły.
2) Termin udzielania odpowiedzi na taką skargę doręczoną przez Prezesa Urzędu wynosi 7 dni (chyba, że Prezes Urzędu wyznaczy inny).

3) Odpowiedź przygotowuje wskazany przez Dyrektora szkoły Pracownik lub Współpracownik a do Prezesa Urzędu ostateczną wersję odpowiedzi uzgodnioną z inspektorem ochrony danych przesyła Dyrektor szkoły lub umocowana przed niego osoba.

5. Zasady przetwarzania danych osobowych w WSCKZiU

1) **Zasada legalności, rzetelności i przejrzystości**

Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Nie wolno przetwarzać danych osobowych bez podstawy prawnej. Przed przystąpieniem do przetwarzania nowej kategorii danych osobowych lub danych w nowym celu należy wskazać podstawę prawną do ich przetwarzania.

2) **Zasada minimalizacji danych**

Dane osobowe muszą być przetwarzane wyłącznie w konkretnym i jasno sprecyzowanym celu, a właściciel danych musi być o tym celu poinformowany. Dane osobowe musza być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

3) **Zasada minimalizacji**

Można zbierać tylko tyle danych, ile jest adekwatne do realizacji celu. Nie można zbierać „na zapas" ze względu na to, że w przyszłości się „przydadzą". Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

4) **Zasada prawidłowości**

Wszystkie osoby upoważnione do przetwarzania i Procesorzy odpowiadają za poprawność merytoryczną danych. Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

5) **Zasada ograniczenia przetwarzania**

Można przetwarzać dane osobowe tylko tak długo jak długo istnieje cel przetwarzania lub określają to przepisy prawa. Dane osobowe muszą być przechowywane w formie

umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

6) **Zasada poufności i integralność**

Dane osobowe muszą być przetwarzane 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.

7) **Zasada zaznajamiania osób upoważnionych z przepisami wewnętrznymi i zewnętrznymi w zakresie ochrony danych osobowych**

Każda osoba upoważniona do przetwarzania danych osobowych (każdy Pracownik i Współpracownik) jest zobowiązany do zapoznawania się na bieżąco z przepisami wewnętrznymi i zewnętrznymi w zakresie ochrony danych osobowych. W przypadku braku wiedzy można skorzystać ze szkolenia / wsparcia inspektora ochrony danych kontaktując się pod adresem: iod@wsckziu.gniezno.pl oraz telefonicznie 601 140 404. Każda osoba upoważniona po zapoznaniu się z przepisami i zasadami w zakresie ochrony danych osobowych, potwierdza ten fakt poprzez pisemne podpisanie stosownego oświadczenia (w tym np. podpisanie oświadczenia o odbyciu szkoleń, o zapoznaniu się z materiałami szkoleniowymi itd.)

8) **Zasada ograniczonego dostępu**

Dostęp do danych osobowych zawsze musi być ograniczony tylko dla osób upoważnionych. Ograniczanie dostępu może być organizacyjne (np. osobiste nadzorowanie, wprowadzanie procedur), fizyczne (np. zamykanie na klucz szafy biurowe, kantorki, drzwi) lub informatyczne (np. stosowanie loginów i haseł).

9) **Zasada podwójnego dostępu**

Dostęp do danych osobowych zawsze musi być ograniczony poprzez zastosowanie minimum **dwóch ograniczeń dostępu** dowolnego rodzaju.

Przykładowe podwójne ograniczenia dostępu:

PIERWSZE OGRANICZENIE DOSTĘPU	DRUGIE OGRANICZENIE DOSTĘPU
• *drzwi do pomieszczeń zamykane na klucz*	• *szafy zamykane na klucz*
• *system IT chroniony loginem i hasłem*	• *zaszyfrowany dodatkowym hasłem nośnik informatyczny*

10) **Zasada czystego biurka**

Po skończonej pracy, na biurku Pracownika / Współpracownika nie mogą się znajdować żadne dokumenty lub ogólnodostępne nośniki informatyczne zawierające dane

osobowe. Wszystkie takie dokumenty / nośniki powinny być zamknięte na klucz w szafach / kantorkach.

11) **Zasada bezpiecznego niszczenia dokumentów i nośników danych**

Usuwanie danych poprzez niszczenie dokumentów w postaci papierowej lub w postaci elektronicznej odbywa się zgodnie z „***Procedurą bezpiecznego usuwania danych osobowych***".

12) **Zasada rozliczalności**

1. Działania osoby upoważnionej lub Procesora na danych osobowych w szczególności w systemach informatycznych muszą być zawsze przypisane w sposób jednoznaczny tylko jednemu Pracownikowi. To oznacza, że dany login do systemu IT może być przypisany TYLKO JENDEJ OSOBIE. **Zakazane jest współdzielenie loginów przez dwie i więcej osób**. Działania przypisane w systemie IT do konkretnego loginu zawsze będę przypisywane osobie, która posługiwała się tym loginem.
2. Wykonując obowiązki i zadania z przepisów RODO oraz niniejszej Polityki, każda osoba upoważniona jest zobowiązana wykazać, że przestrzega przepisów RODO i Polityki.

13) **Zasada tajemnicy i jakości haseł dostępowych**

Pod żadnym pozorem nie wolno ujawnić swojego hasła dostępowego (ani przełożonemu, ani Pracodawcy ani żadnej innej osobie nawet pracownikom organów państwowych). Hasło po otrzymaniu od administratora systemu należy zmienić tego samego dnia. **Hasło musi mieć minimum 8 znaków. Każde hasło należy zmieniać nie rzadziej niż raz na 90 dni.**

6. Zasady powierzania przez WSCKZiU przetwarzania danych osobowych podmiotom trzecim

1) **Stosowanie umów powierzenia**

W przypadku zawierania umowy o świadczenie usług, które jest związane z powierzeniem przetwarzania danych osobowych dostawcy usługi, należy zawrzeć pisemną umowę powierzenia przetwarzania zgodną z art. 28 RODO.

2) **Obowiązki i odpowiedzialności Procesorów**

W trakcie tworzenia umowy powierzenia przetwarzania danych osobowych należy bezwzględnie zapisać następujące kwestie:

a) przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora oraz Procesora,

b) Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – 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 administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny,

c) Procesor zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

d) Procesor podejmuje wszelkie środki wymagane na mocy art. 32 RODO,

e) Procesor nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian,

f) Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania Procesor korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa powyżej, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym,

g) Procesor biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO,

h) Procesor uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO,

i) Procesor po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,

j) Procesor udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych art. 28 RODO oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

3) **Obowiązki i odpowiedzialności osób nadzorujących Procesorów**

Prowadzący merytorycznie daną umowę jest zobowiązany osobiście lub poprzez wyznaczonego pracownika nadzorować Procesora czy spełnia wymagania zawartej umowy powierzenia przetwarzania danych. W przypadku podejrzenia, że Procesor nie wypełnia zapisów Umowy lub Ustawy, należy ten fakt zgłosić zgodnie z ***Procedurą postępowania w przypadku naruszenia przepisów o ochronie danych osobowych***.

4) **Kontrola Procesorów**

W każdej umowie powierzenia przetwarzania danych osobowych, obowiązkowo stosuje się zapis o możliwości przeprowadzenia kontroli (audytu) zgodności przetwarzania powierzonych danych z Umową oraz przepisami. Kontrolę taką może przeprowadzać osoba pisemnie upoważniona przez WSCKZiU osoba.

7. Określenie minimalnych środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych w WSCKZiU.

7.1. Środki organizacyjne zabezpieczenia danych osobowych

W celu wzmocnienia nadzoru nad procesami przetwarzania danych osobowych zostały wprowadzone środki organizacyjne zabezpieczenia danych opisane w niniejszym punkcie.

7.2. Szkolenia wewnętrzne

Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązania do odbycia minimum jednego szkolenia (stacjonarnego, e-learningowego lub innego które wdroży inspektor ochrony danych) raz na rok w zakresie przepisów o ochronie danych osobowych. W zależności od ilości przetwarzanych informacji oraz intensywności jak również rodzaju danych osobowych, które przetwarza osoba- inspektor ochrony danych decyduje o sposobie budowania świadomości tej osoby wybierając właściwą formę szkoleniową.

7.3. Wprowadzanie zasad i procedur

Polityka bezpieczeństwa danych osobowych stanowi podstawę do opracowania i wdrożenia kolejnych procedur ochrony danych osobowych, których za konieczne do wdrożenia uzna inspektor ochrony danych. Niniejsza Polityka wdraża także zasady określone w poszczególnych punktach oraz daje uprawnienia dla dostawcy IT oraz dla inspektora ochrony danych do wdrażania zasad lub wydawania rekomendacji wiążących użytkowników systemów IT.

7.4. Planowanie wykonywania kopii zapasowych zbiorów danych osobowych

Dan osobowe przetwarzane w systemach informatycznych są zabezpieczone za pomocą systemów kopii zapasowych nadzorowanych przez dostawcę IT lub osobę odpowiedzialną za obsługę IT. Systemy te tworzą kopie zapasowe zgodnie z harmonogramem określonym przez dostawcę IT. Plan wykonywania kopii zapasowych dla każdego systemu IT określony jest w odrębnym dokumencie, który tworzy bezpośrednio osoba odpowiedzialna za systemy IT.

7.5. Pełna rejestracja operacji na danych osobowych w powiązaniu z konkretnym użytkownikiem (login)

Każdy system IT użytkowany w WSCKZiU zapewnia, że operacje na danych osobowych można powiązać z konkretnym użytkownikiem. Dotyczy to zarówno części aplikacyjnej systemu oraz części bazodanowej. W przypadku zakupu nowych systemów IT, dostawca IT

zapewnia aby w specyfikacji zakupu systemu IT był zapis o spełnieniu przez dostawcę wymagań dotyczących integralności, poufności rozliczalności wprowadzania i korzystania z danych w systemie.

7.6. Minimalne środki techniczne zabezpieczenia danych osobowych

Opisane w niniejszym punkcie środki techniczne zabezpieczenia danych są stosowane do zborów danych osobowych jednak nie wszystkie do wszystkich zbiorów. W zależności od kategorii, rodzaju, charakteru, celu przetwarzania danych osobowych są stosowane adekwatne środki bezpieczeństwa i zapewniające zgodność przetwarzania z przepisami Rozporządzenia.

7.7. ŚRODKI OCHRONY FIZYCZNEJ DANYCH

1) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy

2) Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są systemem dostępu za pomocą drzwi zamykanych na klucz

3) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy

4) Szafy i kantorki w których składowane są dokumenty zawierające dane osobowe zamykane są na klucz

5) W celu zapewnienia rozliczalności administratora obowiązuje odpowiednia procedura dotycząca pozyskiwania kluczy do pomieszczeń w których przetwarzane są dane osobowe

6) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych

7) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów

8) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

9) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco

7.8. ŚRODKI SPRZĘTOWE INFRASTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ

1) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

2) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.

3) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

4) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

5) Zastosowano zapisy w procedurach dotyczące okresowej zmiany haseł jak chociażby w niniejszej Polityce

7.9. ŚRODKI OCHRONY W RAMACH NARZĘDZI PROGRAMOWYCH I BAZ DANYCH

1) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

2) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

3) Zastosowano kryptograficzne środki ochrony danych osobowych.

4) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

5) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

8. Pozostałe dokumenty określające poziom zabezpieczeń technicznych i organizacyjnych

1) Całkowite, szczegółowe i aktualne zabezpieczenia techniczne i organizacyjne stosowane przez administratora opisane są w oddzielnym dokumencie pn. ***„Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa”.***

9. Inspektor ochrony danych

9.1. Wyznaczenia inspektora ochrony danych

1) WSCKZiU dokonało analizy konieczności wyznaczenia inspektora ochrony danych na mocy art. 37 RODO i stwierdziło, że zachodzą przesłanki jego wyznaczenia

2) WSCKZiU, mając na uwadze ochroną praw i wolności osób w związku z przetwarzaniem danych osobowych, wyznaczyło inspektora ochrony danych. Wyznaczenie odbywać się będzie każdorazowo poprzez wydanie Zarządzenia Dyrektora powołującego i wskazującego imiennie osobę pełniącą funkcję inspektora ochrony danych i może być nią osoba wybrana zarówno spośród obecnych Pracowników lub Współpracowników jak i spoza tego grona.

3) WSCKZiU zapewnia środki na funkcjonowanie inspektora ochrony danych.

4) Zadania inspektora ochrony danych wynikają z niemniejszej Polityki, innych dokumentów dot. ochrony danych osobowych jak również przepisów krajowych dotyczących ochrony danych osobowych oraz RODO.

9.2. Rekomendacje i wsparcie dla inspektora ochrony danych

1)I Inspektor ochrony danych wydaje rekomendacje stosowania przepisów o ochronie danych osobowych.

1) Rekomendacje mogą dotyczyć stosowanych wzorów oświadczeń, formularzy, wzorów dokumentów, umów czy innych zapisów w dokumentach wewnętrznych WSCKZiU dotyczących ochrony danych osobowych.

2) Do inspektora ochrony danych można zwrócić się o przygotowanie nowego rekomendowanego dokumentu / wzoru / zapisu na adres iod@wsckziu.gniezno.pl. W takim przypadku inspektor ochrony danych po zebraniu niezbędnych informacji przygotowuje rekomendowaną treść.

10. Wykaz proponowanych dokumentów (w tym procedur) dotyczących ochrony danych osobowych, które winny być stosowane w WSCKZiU

1) Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych,

2) Procedura bezpiecznego usuwania danych osobowych,

3) Procedura realizacji prawa dostępu do danych osób, których dane dotyczą,
4) Procedura postępowania w przypadku naruszenia przepisów o ochronie danych osobowych
5) Procedura stosowania systemów IT
6) Polityka informacyjna w zakresie wykonywania obowiązku informacyjnego z art. 13 i art. 14 RODO
7) Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa
8) Procedura stosowania monitoringu wizyjnego
9) Wykaz procesów przetwarzania oraz retencji danych osobowych
10) Wykaz budynków, pomieszczeń lub ich części w których przetwarzane są dane osobowe