Polityka ochrony danych osobowych

w

Centrum Kształcenia Ustawicznego

w Zduńskiej Woli

25 maja 2018 r.

Niniejsza *Polityka ochrony danych osobowych*, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w Centrum Kształcenia Ustawicznego w Zduńskiej Woli, ul. Komisji Edukacji Narodowej 6 , 98-220 Zduńska Wola, NIP 829-171-63-38 REGON 100722457, tel. 43 823 62 13, strona internetowa: www.jasna.org.pl email jasna6@op.pl, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L z 2016 r. Nr 119, str. 1), dalej „RODO" oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

Definicje:

1. **Administrator Danych** - Centrum Kształcenia Ustawicznego w Zduńskiej Woli, ul. Komisji Edukacji Narodowej 6 , 98-220 Zduńska Wola, NIP 829-171-63-38 REGON 100722457, tel. 43 823 62 13, strona internetowa: www.jasna.org.pl email jasna6@op.pl,
2. **Organ zarządzający** – podmiot lub organ upoważniony do działania w imieniu i na rzecz Administratora Danych – Dyrektor Centrum Kształcenia Ustawicznego w Zduńskiej Woli.
3. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
4. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji oraz narzędzi programowych zastosowanych w celu przetwarzania danych
5. **Podmiot przetwarzający** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych
6. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów
7. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych
8. **Identyfikator podmiotu przetwarzającego** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (podmiotu przetwarzającego) w razie Przetwarzania danych osobowych w takim systemie
9. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (podmiotowi przetwarzającemu) w razie przetwarzania danych osobowych w takim systemie
10. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (podmiotu przetwarzającego).

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w Centrum Kształcenia Ustawicznego w Zduńskiej Woli, ul. Komisji Edukacji Narodowej 6 , 98-220 Zduńska Wola, NIP 829-171-63-38 REGON 100722457, tel. 43 823 62 13, strona internetowa: www.jasna.org.pl email jasna6@op.pl,, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora Danych przy ul. Komisji Edukacji Narodowej 6, 98-220 Zduńska Wola.
3. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   1) odpowiednie do zagrożeń i kategorii Danych osobowych objętych ochroną środki techniczne i rozwiązania organizacyjne;
   2) kontrolę i nadzór nad Przetwarzaniem Danych osobowych;
   3) monitorowanie zastosowanych środków ochrony.
4. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Podmiotów Przetwarzających, naruszanie zasad dostępu do Danych osobowych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
5. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem Danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u Administratora Danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator Danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator Danych wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator Danych dokonuje analizy ich skutków dla ochrony Danych osobowych oraz uwzględnia kwestie ochrony Danych osobowych w fazie ich projektowania.
4. Administrator Danych prowadzi rejestr czynności przetwarzania.
5. Rejestr czynności przetwarzania stanowi załącznik nr 1 do niniejszej Polityki.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania Danych osobowych zgodnie z obowiązującymi przepisami oraz zgodnie z ustaloną przez Administratora Danych Polityką Ochrony Danych Osobowych, Instrukcją Bezpieczeństwa Przetwarzania Danych

Osobowych, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w Centrum Kształcenia Ustawicznego w Zduńskiej Woli.

2. Wszystkie Dane osobowe są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   1) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania Danych osobowych;
   2) Dane osobowe są przetwarzane rzetelnie i w sposób przejrzysty;
   3) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
   4) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
   5) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane;
   6) Czas przechowywania Danych osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane;
   7) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO;
   8) Dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych Osobowych uważa się w szczególności:
   1) naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są Dane osobowe, w razie ich przetwarzania w takich systemach;
   2) udostępnianie lub umożliwienie udostępniania Danych osobowych osobom lub podmiotom do tego nieupoważnionym;
   3) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
   4) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   5) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
   6) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
   7) naruszenie praw osób, których dane są przetwarzane.
4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony Danych osobowych Podmiot Przetwarzający zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.

5. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy, aby:
    1) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków;
    2) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do Przetwarzania danych osobowych. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszej Polityki. Wzór cofnięcia upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej Polityki.
    3) każdy pracownik zobowiązał się do zachowania w tajemnicy i poufności Danych osobowych przetwarzanych w Zespole Szkół Specjalnych im. Marii Grzegorzewskiej w Zduńskiej Woli. Wzór oświadczenia pracownika stanowi załącznik nr 4 do niniejszej Polityki.
    4) Oświadczenie i zobowiązanie osoby przetwarzającej Dane osobowe do zachowania tajemnicy stanowi element upoważnienia do przetwarzania Danych osobowych.
6. Administrator Danych prowadzi rejestr upoważnień do przetwarzania Danych osobowych stanowiący załącznik nr 5 do niniejszej Polityki.
7. Pracownicy zobowiązani są do:
    1) ścisłego przestrzegania zakresu nadanego upoważnienia;
    2) przetwarzania i ochrony Danych osobowych zgodnie z przepisami;
    3) zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
    4) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
8. Stażyści, wolontariusze oraz praktykanci wykonujący obowiązki na rzecz CKUw Zduńskiej Woli zobowiązani są do zachowania w tajemnicy i poufności Danych osobowych przetwarzanych w CKU w Zduńskiej Woli. Wzór oświadczenia stanowi załącznik nr 6 do niniejszej Polityki.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie CKUw Zduńskiej Woli, obejmuje pomieszczenia zlokalizowane w budynku położonym w Zduńskiej Woli
    1) przy ul. KEN 6, 98-220 Zduńska Wola,

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

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych Danych osobowych.

2. Zastosowane środki ochrony techniczne i organizacyjne powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii Danych osobowych.
3. Środki ochrony techniczne i organizacyjne obejmują:
   1) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania Danych Osobowych jedynie w towarzystwie osoby upoważnionej;
   2) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt IV na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich;
   3) wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów;
   4) wykorzystanie odpowiedniej niszczarki (sposób niszczenia - sieczka) do skutecznego usuwania dokumentów zawierających Dane osobowe;
   5) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall;
   6) wykonywanie kopii awaryjnych Danych osobowych na nośnikach danych zewnętrznych/serwer należący do Administratora Danych;
   7) ochronę sprzętu komputerowego wykorzystywanego u Administratora Danych przed złośliwym oprogramowaniem;
   8) zabezpieczenie dostępu do urządzeń przy pomocy haseł dostępu (komputerów stacjonarnych i przenośnych, telefonów komórkowych);
   9) wykorzystanie szyfrowania danych przy ich transmisji.
4. W ramach środków ochrony technicznych oraz organizacyjnych wprowadza się Politykę czystego biurka stanowiącą załącznik nr 7 do niniejszej Polityki.
5. W ramach środków ochrony technicznych oraz organizacyjnych systemów komputerowych, Administrator Danych wprowadza Instrukcję bezpieczeństwa przetwarzania danych osobowych stanowiącą załącznik nr 8 do niniejszej Polityki.
6. Administrator Danych wprowadza Procedurę ws. poczty elektronicznej stanowiącą załącznik nr 9 do niniejszej Polityki.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Administrator Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Formularz oceny naruszenia Danych osobowych stanowi załącznik nr 10 do niniejszej Polityki.
2. Stwierdzenie naruszenie ochrony Danych osobowych winno zostać dokonane w formie Formularza wykrycia naruszenia stanowiącego załącznik nr 11 do niniejszej Polityki.
3. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych zgłasza fakt naruszenia zasad

ochrony Danych osobowych organowi nadzorczemu bez zbędnej zwłoki – jeżeli jest to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych stanowi załącznik nr 12 do niniejszej Polityki.

4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator Danych zawiadamia o incydencie także osobę, której dane dotyczą, zgodnie z art. 34 ust. 1 RODO. Wzór zawiadomienia stanowi załącznik nr 13 do niniejszej Polityki.
5. W przypadku, gdy stwierdzono naruszenia ochrony Danych osobowych, a jest mało prawdopodobne, aby naruszenia skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator Danych nie dokonuje zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, o którym mowa w pkt VI ust. 2, zgodnie z art. 33 ust. 1 RODO.
6. Administrator Danych prowadzi rejestr naruszeń ochrony danych osobowych, który stanowi załącznik nr 14 do niniejszej Polityki.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych może powierzyć Przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
2. Przed powierzeniem Przetwarzania danych osobowych, Administrator Danych w miarę możliwości uzyskuje informacje o dotychczasowych praktykach przetwarzającego, dotyczących zabezpieczenia danych osobowych.
3. Wzór umowy powierzenia danych, o której mowa w pkt VII ust. 1 stanowi załącznik nr 15 do niniejszej Polityki.

VIII. Przekazywanie danych do państwa trzeciego

Administrator Danych nie będzie przekazywał Danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

IX. Polityka informacyjna oraz prawa osób, których dane dotyczą

1. Zgodnie z art. 13 ust. 1 RODO, Administrator Danych w celu realizacji obowiązku informacyjnego osób, których dane dotyczą, wprowadza klauzulę informacyjną.
2. Klauzula informacyjna stanowi załącznik nr 16 do niniejszej Polityki.

X. Procedura realizacji praw osób, których dane dotyczą

1. W celu ochrony i realizacji praw osób, których dane dotyczą, wskazanych w RODO, Administrator Danych wprowadza Procedurę Realizacji Praw Osób, Których Dane Dotyczą, stanowiącą załącznik nr 17 do niniejszej Polityki.
2. Administrator Danych tworzy rejestr zgłoszeń osób, których dane dotyczą. Wzór rejestru osób, których dane dotyczą stanowi załącznik nr 18 do niniejszej Polityki.
3. Administrator Danych otrzymaniu zgłoszenia osoby, której dane dotyczą, w zakresie realizacji praw wynikających z RODO, rozpatruje przedmiotowe zgłoszenie, a następnie zawiadamia wskazaną osobę o podjętych działaniach oraz rozstrzygnięciu sprawy,

przede wszystkim o sprostowaniu, usunięciu oraz ograniczeniu przetwarzania, zgodnie z art. 19 RODO.

XI. Inspektor Ochrony Danych

1. Administrator Danych wyznaczy Inspektora Ochrony Danych, zwanego dalej IOD.
2. Funkcję IOD można zlecić jednostkom zależnym lub stronom trzecim. Aby być skutecznym, Inspektor Ochrony Danych powinien mieć jasno określony zakres obowiązków, odpowiednio usytuowany w strukturze organizacyjnej jako niezależna funkcja i niezbędna część systemu kontroli wewnętrznej. Inspektor Ochrony Danych podlega bezpośrednio organowi zarządzającemu. Administrator Danych zapewnia, aby zajmowane stanowisko i zakres obowiązków Inspektora Ochrony Danych nie powodowały konfliktu interesów.
3. Do zadań Inspektora Ochrony Danych należy w szczególności:
   1) informowanie Administratora Danych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają Dane Osobowe, o obowiązkach spoczywających na nich na mocy niniejszej Polityki oraz obowiązujących przepisów i regulacji w zakresie ochrony danych osobowych;
   2) monitorowanie przestrzegania niniejszej Polityki oraz obowiązujących przepisów i regulacji w zakresie ochrony danych osobowych oraz polityk Przetwarzającego w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty, przyjmując również podejście oparte na ryzyku;
   3) informowanie organu zarządzającego, że wymagana jest ocena skutków ochrony danych osobowych, a po osiągnięciu porozumienia w sprawie takiego wymogu, udzielanie porad w odniesieniu do oceny skutków ochrony danych osobowych (czy należy przeprowadzić ocenę skutków ochrony danych osobowych, jaką metodologię zastosować, niezależnie od tego, czy należy przeprowadzić wewnętrzną ocenę skutków lub wewnętrznie ją zlecić, jakie zabezpieczenia zostaną zastosowane w celu ograniczenia wszelkiego ryzyka dla praw i wolności osób, których dane dotyczą) oraz monitorowanie jej wyników (niezależnie od tego, czy oceny skutków ochrony danych osobowych została prawidłowo przeprowadzona, czy w międzyczasie można prowadzić działania związane z przetwarzaniem danych osobowych i jakie środki bezpieczeństwa należy przyjąć oraz czy ich wnioski są zgodne z przepisami ustawowymi i wykonawczymi w zakresie ochrony danych);
   4) współpraca z organem nadzorczym;
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
4. Organ zarządzający zapewnia, że IOD jest niezależny. W celu zachowania swojej niezależności, Inspektor Ochrony Danych:
   1) nie może otrzymywać instrukcji dotyczących wykonywania swoich zadań;
   2) nie może zostać zwolniony lub ukarany za wypełnianie swoich zadań;

3) nie można wydawać mu wiążących poleceń co do załatwienia konkretnej sprawy, jakie wyniki należy osiągnąć, jak zbadać skargę lub skonsultować się z organem nadzoru, czy też co do treści opinii związanej z prawem ochrony danych osobowych lub jakąkolwiek konkretną interpretacją prawa;
4) ma prawo wyrazić zdanie odrębne w przypadku decyzji, które są niezgodne z prawem o ochronie danych osobowych lub z jego radą/opinią; w przypadku, gdy organ zarządzający nie zgadza się z radą/opinią Inspektora Ochrony Danych, obowiązany jest do należytego udokumentowania i uzasadniania przyczyn nieprzestrzegania zaleceń Inspektora Ochrony Danych.

5. Inspektor ochrony danych musi posiadać wiedzę specjalistyczną w zakresie:
   1) krajowych i europejskich przepisów i praktyk w zakresie ochrony danych;
   2) operacji przetwarzania danych osobowych prowadzonych przez Administratora Danych;
   3) zasad i procedur obowiązujących u Administratora Danych;
   4) przedmiotu działalności i branży, w której działa Administrator Danych.
6. Inspektor Danych Osobowych:
   1) tworzy wytyczne i procedury operacyjne dotyczące wdrożenia zasad dotyczących danych osobowych,
   2) definiuje metodologię, którą należy zastosować (w razie potrzeby) w odniesieniu do operacji przetwarzania danych osobowych;
   3) we współpracy z organem zarządzającym prowadzi kontrole w zakresie oceny zagadnień związanych z ochroną danych osobowych;
   4) jest systematycznie angażowany na najwcześniejszym etapie we wszystkie kwestie związane z ochroną danych osobowych;
   5) jest niezwłocznie informowany o naruszeniu Danych Osobowych lub innym incydencie;
   6) udziela porad w przypadku przeprowadzenia oceny skutków dla ochrony danych;
   7) działa jako punkt kontaktowy dla organu nadzoru w kwestiach związanych z Przetwarzaniem, w tym w ramach wcześniejszych konsultacji i konsultowania, w razie potrzeby, w odniesieniu do każdej innej kwestii;
   8) pełni rolę punktu kontaktowego dla osób, których dane dotyczą np. w przypadku wykonywania ich praw.

XII. Postanowienia końcowe

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu, pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, ustawy o ochronie danych osobowych oraz Kodeksu karnego, w związku z naruszeniem zasad oraz obowiązków dotyczących przetwarzania danych osobowych.

XIII. Załączniki

1. Załącznik nr 1 - Rejestr czynności przetwarzania.
2. Załącznik nr 2 - Wzór upoważnienia do przetwarzania danych osobowych.
3. Załącznik nr 3 - Wzór cofnięcia upoważnienia do przetwarzania danych osobowych.
4. Załącznik nr 4 - Wzór oświadczenia pracownika.

5. Załącznik nr 5 - Rejestr upoważnień do przetwarzania danych osobowych.
6. Załącznik nr 6 - Wzór oświadczenia stażysty, wolontariusza oraz praktykanta.
7. Załącznik nr 7 - Polityka czystego biurka.
8. Załącznik nr 8 - Instrukcja bezpieczeństwa przetwarzania danych osobowych.
9. Załącznik nr 9 - Procedura ws. poczty elektronicznej.
10. Załącznik nr 10 - Formularz oceny naruszenia danych osobowych.
11. Załącznik nr 11 - Formularz wykrycia naruszenia.
12. Załącznik nr 12 - Wzór zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.
13. Załącznik nr 13 - Wzór zawiadomienia osoby, której dane dotyczą, o naruszenia ochrony danych osobowych.
14. Załącznik nr 14 - Rejestr naruszeń ochrony danych osobowych.
15. Załącznik nr 15 - Wzór umowy powierzenia przetwarzania.
16. Załącznik nr 16 - Klauzula informacyjna.
17. Załącznik nr 17 - Procedura realizacji praw osób, których dane dotyczą.
18. Załącznik nr 18 - Rejestr zgłoszeń osób, których dane dotyczą.

Załącznik nr 8
do Polityki Ochrony Danych Osobowych
w Centrum Kształcenia Ustawicznego
w Zduńskiej Woli

INSTRUKCJA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH wprowadzona w Centrum Kształcenia Ustawicznego w Zduńskiej Woli.

§ 1.

Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym.

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych.
2. Upoważnienia do przetwarzania danych osobowych, o których mowa w § 1 ust. 1 przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po:
   1) podaniu identyfikatora użytkownika i właściwego hasła w przypadku programów informatycznych przeznaczonych do przetwarzania danych osobowych,
   2) podaniu właściwego hasła dostępu do stanowiska komputerowego.
4. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Danych ustala niepowtarzalny identyfikator i hasło początkowe.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
6. W przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest Administrator Danych.

§ 2.

Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów niestacjonarnych.
2. Hasło użytkownika powinno mieć minimum 8 znaków i być zmieniane w przypadku :
   1) Programów informatycznych przeznaczonych do przetwarzania danych osobowych co 30 dni,
   2) dostępu do stanowiska komputerowego co 90 dni.

3. Hasło oprócz znaków małych i dużych liter winno zawierać ciąg znaków alfanumerycznych i specjalnych.
4. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej.
5. Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.
6. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej.
7. Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności.
8. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
9. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym Administratora Danych.

§ 3.
Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

1. Dane osobowe, których administratorem jest Centrum Kształcenia Ustawicznego w Zduńskiej Woli, mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby związane z działalnością Administratora Danych.
2. Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).
3. Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji.
4. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji
5. Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.
6. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.
7. Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika.
8. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce dokumentów.

9. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
10. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.
11. Użytkownik niezwłocznie powiadamia Administratora Danych w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

§ 4.
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania.

1. Dane osobowe w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą sporządzanie kopii zapasowych (kopie pełne).
2. Pełne kopie zapasowe tworzone są 2 razy w ciągu roku.
3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
4. Kopie zapasowe należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu.
5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

§ 5.
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1. Okresowe kopie zapasowe wykonywane są na płytach CD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie w szafie zamykanej na klucz.
2. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma Administrator Danych.
3. Kopie miesięczne przechowuje się przez okres 6 miesięcy. Wykonywane co pół roku pełne kopie systemu kadrowego przechowuje się przez 50 lat. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
5. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.
6. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.

§ 6.

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W związku z istnieniem zagrożenia dla danych osobowych, ze strony wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.
2. Wirusy komputerowe mogą pojawić się systemach poprzez: Internet, nośniki informacji takie jak: dyskietki, płyty CD, dyski przenośne, itp.
3. Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:
   1) Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego.
   2) Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz co najmniej raz w tygodniu dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
   3) Elektroniczne nośniki informacji należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Danych.
   4) Komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).
   5) W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem.
   6) Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców.
   7) Zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

§ 7.

Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych

Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa.

§ 8.

Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje systemu wykonuje na bieżąco Administrator Danych lub osoba wskazana/ upoważniona przez administratora.

2. Administrator Danych okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.

3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku.

4. Naprawy sprzętu należy zlecać podmiotom, których kompetencje nie budzą wątpliwości, co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz Administratora w miejscu jego użytkowania.

5. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.

6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Danych.

§ 9.
Ustalenia końcowe

1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe zabrania się:
   1) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
   2) pozostawiania haseł w miejscach widocznych dla innych osób,
   3) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
   4) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
   5) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
   6) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
   7) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza budynek Centrum Kształcenia Ustawicznego w Zduńskiej Woli,
   8) samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są przez Administratora,
   9) używania nośników danych udostępnionych przez osoby postronne,
   10) przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (nie służbowego),
   11) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców,
   12) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia

niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia - przeskanowania programem antywirusowym, Administratorowi Danych,

13) tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania,
14) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
15) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
16) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
17) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach placówki, w których przetwarzane są dane osobowe,
18) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
19) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
20) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,
21) ignorowania zapisów Polityki Bezpieczeństwa.

2. W związku z przetwarzaniem danych w systemie informatycznym konieczne jest:
1) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
2) tworzenia haseł trudnych do odgadnięcia dla innych,
3) traktowanie konta pocztowego jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,
4) nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
5) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
6) zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych.
3. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Danych lub bezpośredniemu przełożonemu.
4. Dane kontaktowe Administratora Danych:
Centrum Kształcenia Ustawicznego w Zduńskiej Woli, ul. Komisji Edukacji Narodowej 6, 98-220 Zduńska Wola, NIP 8291716338, REGON 100722457, tel. 43 823 62 13, strona internetowa: www.jasna.org.pl, email: jasna6@op.pl

§ 10.

Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia biurowe.
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w § 10 ust. 1, nie można wynosić poza teren przetwarzania danych, tj. siedzibę Administratora Danych.
4. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania administrator o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

§ 11.
Obowiązki Administratora Danych Osobowych

1. Administrator Danych zobowiązany jest do zapewnienia, aby dane osobowe były:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów,
   3) merytorycznie poprawne i adekwatne w stosunku do celów.
2. Administrator Danych opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
3. Administrator Danych określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
4. Administrator Danych opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
5. Administrator Danych prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
6. Administrator Danych organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
7. Administrator Danych odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:
   1) ochronę danych przed niepowołanym dostępem,
   2) nieuzasadnioną modyfikację lub zniszczenie danych,
   3) nielegalne ujawnienie danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

§ 12.
Obowiązki Inspektora Ochrony Danych

Inspektor Ochrony Danych obowiązany jest do:

1) Nadzoru nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.
2) Nadzoru nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
3) Nadzoru nad wykorzystywanym oprogramowaniem oraz jego legalnością.
4) Przeciwdziałania dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe.
5) Podejmowania odpowiednich działań w celu właściwego zabezpieczenia danych.
6) Badania ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.
7) Podejmowania decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
8) Nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
9) Definiowania użytkowników i haseł dostępu.

10) Aktualizowania oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.
11) Nadzoru nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
12) Wdrożenia szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

Załącznik nr 16
do Polityki Ochrony Danych Osobowych
w Centrum Kształcenia Ustawicznego
w Zduńskiej Woli

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L z 2016 r. nr 119 str. 1), dalej RODO, informujemy, iż:

1. Administratorem Danych Pana/Pani danych osobowych (dalej „dane osobowe") jest Centrum Kształcenia ustawicznego w Zduńskiej Woli, ul. Komisji Edukacji Narodowej 6, 98-220 Zduńska Wola, NIP 8291716338, REGON 00722457, tel. 43 823 6213, strona internetowa: , email: jasna6@op.pl
2. Inspektorem Ochrony Danych w Centrum Kształcenia Ustawicznego jest AGNIESZKA RATAJCZAK
3. Administrator Danych przetwarza dane osobowe uczniów, rodziców oraz opiekunów prawnych w celu realizacji zadań wynikających z ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz.U. z 2018 r. poz. 650 ze zm.), m.in. przyjęcia słuchacza do szkoły, realizacja zadań oświatowych, zapewnienia bezpieczeństwa ucznia w czasie pobytu w szkole, umożliwienia słuchaczowi korzystania z pełnej oferty szkoły, a także w związku z utrzymaniem i zapewnieniem bezpieczeństwa systemu informatycznego, w którym przetwarzana jest wszelka dokumentacja związana z procesem rekrutacji.
4. Przetwarzanie danych osobowych ww. celach nie wymaga uzyskania zgody osoby, której dane dotyczą.
5. Podstawą prawną przetwarzania Państwa jest art. 6 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – (dalej: RODO) w zw. z ustawą z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz.U. z 2018 r. poz. 650 ze zm.), ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz.U. z 2017 r. poz. 2198 ze zm.), rozporządzenia Ministra Edukacji Narodowej z dnia 9 sierpnia 2017 r. w sprawie zasad organizacji i udzielania pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach (Dz.U. z 2017 r. poz. 1591 ze zm.) oraz ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz.U. z 2017 r. poz. 2159 ze zm.)
6. Podstawą przetwarzania danych w zakresie, jaki jest niezbędny do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, może być również art. 6 ust. 1 lit. f RODO.
7. W zakresie, w jakim przetwarzane dane obejmują dane szczególnych kategorii, podstawą prawną przetwarzania danych jest art. 9 ust. 2 lit. g RODO.

8. Podanie danych osobowych wynikających z przepisu prawa jest wymogiem ustawowym. Niepodanie tych danych spowoduje brak możliwości realizacji zadań przez Centrum Kształcenia Ustawicznegow Zduńskiej Woli.
9. W przypadku danych osobowych, których przetwarzanie nie wynika wprost z przepisów szczególnych, na przykład wykorzystanie wizerunku uczniów, **koniecznym będzie wyrażenie przez Państwa zgody na przetwarzanie danych osobowych zgodnie z art. 6 ust. 1 lit. a RODO.**
10. Wskazana zgoda może zostać cofnięta w każdej chwili, z zastrzeżeniem, że cofnięcie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania danych przed cofnięciem zgody.
11. Dane osobowe pracowników są przetwarzane w celu realizacji umowy o pracę, a także w związku z obowiązkami wynikającymi z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2018 r. poz. 917 ze zm.) oraz innymi przepisami szczególnymi.
12. Dane wolontariuszy oraz praktykantów przetwarzane są w celu realizacji wolontariatu oraz praktyk na podstawie ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz.U. z 2018 r. poz. 450 ze zm.) oraz innymi przepisami szczególnymi.
13. Dane stażystów przetwarzane są w celi realizacji umowy o organizację stażu na postawie ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz.U. z 2018 r. poz. 1265 ze zm.) oraz innymi przepisami szczególnymi.
14. Przysługuje Pani/Panu prawo dostępu do treści swoich danych osobowych, prawo ich sprostowania, ograniczenia przetwarzania, usunięcia, nie przysługuje Pani/Panu prawo do ich przenoszenia oraz wniesienia sprzeciwu. Jeżeli przetwarzanie danych osobowych odbywa się na podstawie Państwa zgody, mają Państwo prawo cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
15. Odbiorcami danych osobowych mogą być podmioty przetwarzające dane osobowe na zlecenie Administratora lub inne podmioty, których udział w realizacji celów, o których mowa w pkt 3, 6, 7, 9, 11 i 12 jest niezbędne, a także podmioty uprawnione na podstawie obowiązujących przepisów.
16. Dane osobowe będą przechowywane przez okres niezbędny do realizacji celów, o których mowa w pkt 3, 6, 7, 9, 11 i 12 oraz przez okres wynikający z przepisów szczególnych.
17. Pani/Pana dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.
18. Wszelkie informacje i wątpliwości dotyczące przetwarzania Pani/Pana danych osobowych można kierować do Administratora Danych lub Inspektora Ochrony Danych:
    1) w formie pisemnej na adres – ul. Komisji Edukacji Narodowej 6, 98-220 Zduńska Wola,
    2) telefonicznie pod numerem – 43 823 62 13,
    3) mailowo na adres – jasna6@op.pl
19. Jeśli uznaje Pani/Pan, że przetwarzanie danych osobowych narusza przepisy RODO, przysługuje Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa, tel. 22 531 03 00, 606-950-000.