POLITYKA OCHRONY DANYCH OSOBOWYCH

	Funkcja	Imię i Nazwisko	Data /podpis
Opracowała	Inspektor Ochrony Danych	Magdalena Wójcik	
Zatwierdził	Dyrektor ZSI w Kielcach	Tomasz Kozieł	
Właściciel:	Administrator danych: Zespół Szkół Informatycznych im. *gen. Józefa Hauke Bosaka* z siedzibą ul. Warszawska 96, 25 - 401 Kielce	Obowiązuje od: 03.09.2018 r.	

Administrator Danych –
Zespół Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach
reprezentowany przez Dyrektora Szkoły Tomasza Kozieł

dnia 24.05.2018 r. w podmiocie o nazwie:

Zespół Szkół Informatycznych im. *gen. Józefa Hauke Bosaka* z siedzibą ul. Warszawska 96, 25 - 401 Kielce

zgodnie z rozporządzeniem 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

wdraża dokument o nazwie „Polityka Ochrony Danych Osobowych".

Postanowienia tego dokumentu wchodzą w życie z dniem 25.05.2018 r.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych (dalej „Polityka") w podmiocie: określa zasady przetwarzania danych osobowych, oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych, oraz w systemach informatycznych. Niniejsza Polityka bezpieczeństwa przetwarzania danych osobowych została wdrożona w Zespole Szkół Informatycznych im. Gen. Józefa Hauke Bosaka w Kielcach z siedziba ul. Warszawska 96, 25-401 Kielce i opisuje szczegółowe zasady ochrony i nadzoru nad przetwarzaniem danych osobowych.

Każde naruszenie zasad Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnych o współpracy i może skutkować konsekwencjami, zgodnie z Kodeksem Pracy lub odpowiednimi przepisami regulującymi zasady współpracy, jak również odpowiedzialnością przewidzianą w ustawie o ochronie danych osobowych.

I. INFORMACJE OGÓLNE:

a. Administratorem Danych w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach z siedzibą ul. Warszawska 96, 25 - 401 Kielce**,** NIP: 657-17-48-539 jest Dyrektor Szkoły Pan Tomasz Kozieł.
b. Zespół Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach z siedzibą ul. Warszawska 96, 25 - 401 Kielce działa na podstawie Ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz. U z 2004 r. Nr 256, poz 2572, z późn. zm. (Dz. U. z 2017 r. poz. 2198, 2203 i 2361)).
c. Powołano Inspektora Ochrony Danych Osobowych. Jest nim Pani Anna Rubinkiewicz. Kontakt do IOD poprzez e-mail: abcrodo@op.pl; tel: 602-779-754
d. Przez bezpieczeństwo danych osobowych przetwarzanych w Podmiocie Administratora danych należy rozumieć zapewnienie ich poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności oraz niezawodności na odpowiednim poziomie.

II. TERMINOLOGIA:

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań,
Dane szczególnie chronione - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących odpowiedzialności karnej, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym,
Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
Administrator danych (ADO) – Zespół Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach z siedzibą ul. Warszawska 96, 25 - 401 Kielce reprezentowany przez Dyrektora placówki, który decyduje o celach i środkach przetwarzania danych osobowych,
Administrator ochrony systemu informatycznego (ASI) rozumie się osobę odpowiedzialną za funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony stosowanych w systemie,
Inspektor Ochrony Danych (IOD) – osoba lub podmiot wyznaczony przez ADO, nadzorujący przestrzeganie zasad ochrony danych osobowych
Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
nośniki danych osobowych – dyskietki, płyty CD lub DVD, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi,
Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
Hasło - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
Odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą,
Osoba upoważniona do przetwarzania danych osobowych - rozumie się przez to pracownika Zespołu Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach, który upoważniony został na piśmie do przetwarzania danych osobowych przez Dyrektora Zespołu Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach
Uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu
Użytkownik - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło,
Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
Integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Poufność – oznacza zapewnienie, że informacja nie jest udostępniana lub ujawniana /nieupoważnionym osobom, podmiotom lub procesom.
Dostępność – oznacza zapewnienie osiągalności lub możliwości do wykorzystania na żądanie, w założonym czasie przez uprawniony podmiot.
Autentyczność – oznacza zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów).
Niezaprzeczalność – oznacza zapewnienie braku możliwości wyparcia się swojego uczestnictwa w całości lub w części przetwarzania danych przez jeden z podmiotów uczestniczących w przetwarzaniu

Sposób przechowywania, udostępniania i modyfikacji Polityki

Polityka została zatwierdzona w Podmiocie Administratora danych jako dokument obowiązujący.

Niniejszy dokument jest przechowywany i aktualizowany w wersji elektronicznej i papierowej ze względu na czytelność i różnorodność obszarów w których przetwarzane są dane osobowe. Jest on regularnie przeglądany i aktualizowany przez Administratora Danych, oraz przez Inspektora Ochrony Danych.

Zmiany w dokumencie Polityki oraz załącznikach wprowadzane są w chwili pojawienia się ważnych okoliczności lub nowego przepisu, istotnego dla spójności i aktualności Polityki, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora Danych.

Informacje o zmianach podawane są do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez publikację w intranecie lub dokumentach formalnych udostępnianych w ustalony wewnętrznie sposób.

W przypadku zatwierdzenia nowej wersji Polityki jest ona drukowana, a wydruk dołączany jest do prowadzonej dokumentacji ochrony danych osobowych. Załączniki mogą być przechowywane wyłącznie w formie elektronicznej. Ich wydruk następuje tylko w razie zaistnienia takiej konieczności, na zlecenie Administratora Danych lub Inspektora Ochrony Danych.

Dokument Polityki, wraz z załącznikami, stanowi tajemnicę Podmiotu Administratora Danych i jest klasyfikowany jako dokument wewnętrzny.

Zmiany i udostępnianie tekstu Polityki

1. Dopuszcza się dokonywanie zmian w niniejszym dokumencie oraz dokumentach powiązanych tylko przez osoby upoważnione, na zasadach opisanych w Polityce.
2. Tekst niniejszej Polityki wraz z załącznikami zostanie udostępniony osobom przetwarzającym dane w intranecie Administratora danych, aby mogły się one z nim zapoznać i postępować zgodnie z jej postanowieniami.

Znajomość Polityki

Do zapoznania się z niniejszym dokumentem Polityki oraz stosowania zawartych w niej zasad zobowiązane są wszystkie osoby przetwarzające dane osobowe w Zbiorze danych osobowych administrowanym przez Administratora danych.

III. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH:

IV. Strategia bezpieczeństwa i zasady przetwarzania danych.
Analiza ryzyka i uzasadnienie dla zastosowania określonych założeń bezpieczeństwa
danych osobowych;
Standardy zabezpieczeń

V. Procedury i sposoby zagwarantowania realizacji praw osób, których dane są przetwarzane;

VI. Ogólne zasady obowiązujące przy przetwarzaniu danych osobowych

VII. Instrukcja postępowania w przypadku naruszania ochrony danych osobowych

VIII. Kontrola przetwarzania i stanu zabezpieczenia danych osobowych

IX. Rejestr operacji przetwarzania danych osobowych w Zespole Szkół Informatycznych w Kielcach

X. Polityka monitorowania i reagowania na naruszenia ochrony danych w Zespole Szkół Informatycznych w Kielcach

XI. Procedury zarządzania użytkownikami i dostępem do danych

1)Zasady powoływania i funkcjonowania Inspektora Ochrony Danych Osobowych.

1) Rejestr operacji przetwarzania danych osobowych.
2) Rejestr czynności przetwarzania danych osobowych
3) Polityka monitorowania i reagowania na naruszenia ochrony danych.
4) Rejestr incydentów.
5) Procedury zarządzania użytkownikami i dostępem do danych.
    a) Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
    b) Ewidencja osób upoważnionych do przetwarzania danych osobowych;
    c) Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
    d) Wzór oświadczenia o zachowaniu poufności;
    e) Wzór upoważnień otrzymanych od Uczniów/Rodziców/Opiekunów Prawnych/Pracowników;
    f) Wzory Zgód otrzymanych od uczniów, pracowników
    g) Procedura wyboru i weryfikacji podmiotu przetwarzającego dane;
    h) Wykaz podmiotów przetwarzających dane na zlecenie administratora danych.
    i) Środki techniczne i organizacyjne niezbędne dla zapewnienia

poufności, integralności i rozliczalności przetwarzanych danych osobowych.

j) Spełnienie obowiązków informacyjnych Klauzule informacyjne

6) Sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

7) Protokół z kontroli i czynności sprawdzających w zakresie ochrony danych osobowych.

IV. Strategia bezpieczeństwa i zasady przetwarzania danych. Analiza ryzyka i uzasadnienie dla zastosowania określonych założeń bezpieczeństwa danych osobowych w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25 - 401 Kielce

Ankieta ryzyka

Pytania dotyczące charakteru przetwarzanych danych osobowych:

Czy przetwarzanie może skutkować:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
dyskryminacją	X			
kradzieżą tożsamości lub oszustwem dotyczącym tożsamości		X		
stratą finansową	X			
naruszeniem dobrego imienia		X		
naruszeniem poufności danych osobowych chronionych tajemnicą zawodową		X		
wszelką inną znaczną szkodą gospodarczą lub społeczną		X		

Pytania dotyczące kwestii organizacyjno-technicznych:

Czy w odniesieniu do przetwarzanych danych osobowych:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
istnieje ryzyko dostępu osób trzecich do dokumentacji papierowej zawierającej dane osobowe w godzinach pracy ZSI w Kielcach		X		
istnieje ryzyko dostępu osób trzecich do dokumentacji		X		

elektronicznej zawierającej dane osobowe w godzinach pracy ZSI w Kielcach				
istnieje ryzyko dostępu osób trzecich do dokumentacji papierowej zawierającej dane osobowe poza godzinami pracy ZSI w Kielcach		X		
istnieje ryzyko dostępu osób trzecich do dokumentacji elektronicznej zawierającej dane osobowe poza godzinami pracy ZSI w Kielcach		X		
istnieje ryzyko wyniesienia dokumentacji zawierającej dane osobowe poza budynek ZSI w Kielcach		X		
istnieje ryzyko skopiowania przez osobę trzecią dokumentów zawierających dane osobowe ZSI w Kielcach		X		
istnieje ryzyko kradzieży dokumentów zawierających dane osobowe ZSI w Kielcach		X		
istnieje ryzyko zagubienia dokumentów zawierających dane osobowe ZSI w Kielcach		X		
istnieje ryzyko stosowania przez osoby trzecie podsłuchu bezpośredniego lub akustycznego z wykorzystaniem mikrofonów kierunkowych lub instalacji technicznych		X		
istnieje ryzyko zagubienia elektronicznych nośników danych zawierających dane osobowe ZSI w Kielcach		X		

Pytania dotyczące zabezpieczenia sprzętu elektronicznego:

Czy w odniesieniu do przetwarzanych danych osobowych:	BRAK RYZYKA	ZNIKOME RYZYKO	ŚREDNIE RYZYKO	WYSOKIE RYZYKO
istnieje ryzyko włamania do systemu poprzez podszycie się pod uprawnionego użytkownika		X		
istnieje ryzyko nieuprawnionego instalowania urządzeń służących do naruszenia poufności przetwarzanych		X		
istnieje ryzyko nieuprawnionej, świadomej modyfikacji oprogramowania zainstalowanego na komputerze pracownika przez osoby trzecie		X		
istnieje ryzyko użycia oprogramowania zainstalowanego na komputerach pracowników w nieuprawniony sposób		X		
istnieje ryzyko korzystania z nielicencjonowanego oprogramowania na komputerach pracowników		X		
istnieje ryzyko przeglądania (przeszukiwania) pamięci operacyjnej i zewnętrznej komputerów w celu uzyskania określonych informacji			X	
istnieje ryzyko wykorzystania pozostawionych na dysku twardym komputera plików roboczych wytworzonych przez oprogramowanie			X	
istnieje ryzyko skopiowania/kradzieży danych		X		

osobowych podczas wykonywania napraw i konserwacji komputerów				
istnieje ryzyko przypadkowej zmiany ustawień konfiguracyjnych na komputerach			X	
istnieje ryzyko nieupoważnionego uruchomienia komputera z nośnika zewnętrznego (ominięcie mechanizmów bezpieczeństwa systemu operacyjnego i systemu plików NTFS i odczytanie zawartości przetwarzanych dokumentów)		X		

Szacowanie poziomu ryzyka

$$\text{Poziom ryzyka} = \frac{0 \times BR + 0{,}5 \times ZR + 1 \times ŚR + 1{,}5 \times WR}{\text{liczba czynników ryzyka}}$$

gdzie: BR – brak ryzyka, ZR – znikome ryzyko, ŚR – średnie ryzyko, WR – wysokie ryzyko

Skala oceny:

0 - 0,25 – brak ryzyka
0,26 - 0,75 – znikome ryzyko
0,76 – 1,25 – średnie ryzyko
1,26 - 1,5 – wysokie ryzyko

Wnioski:

Ogólny poziom ryzyka związanego z przetwarzaniem danych osobowych oszacowany został:

1) Dla postępowań dotyczących charakteru przetwarzanych danych osobowych – **poziom 0,33**
2) Dla postępowań dotyczących kwestii organizacyjno-technicznych – **poziom 0,50**
3) Dla postępowań dotyczących zabezpieczenia sprzętu elektronicznego – **poziom 0,65**

Najważniejsze ryzyko związane z naruszeniem bezpieczeństwa danych osobowych związane jest z przetwarzaniem danych osobowych w zakresie postępowań prowadzonych w przedmiocie: **Dla postępowań dotyczących zabezpieczenia sprzętu elektronicznego** - Związane jest to przede wszystkim z charakterem przetwarzanych danych, sposobem przetwarzania danych przez personel oraz obsługą systemu informatycznego w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25 - 401 Kielce**.**

Najważniejszymi obszarami wymagającymi weryfikacji celem minimalizacji poziomu ryzyka są: **usystematyzowanie kwestii organizacyjno-technicznych oraz zabezpieczenia sprzętu elektronicznego dla zwiększenia ochrony danych przechowywanych w systemie informatycznym.**

Po przeprowadzeniu ankiety ryzyka i oszacowaniu poziomu ryzyka proponuje się podjęcie działań w zakresie zwiększenia bezpieczeństwa danych osobowych przetwarzanych

w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25 - 401 Kielce poprzez:

Lp	Nazwa	Konieczność	Brak konieczności
1	Wprowadzenie dodatkowych zabezpieczeń w zakresie organizacyjno-technicznym		
2	Wprowadzenie dodatkowych zabezpieczeń komputerów poprzez wprowadzenie haseł do sieci wewnętrznej.		
3	Zakup nowego oprogramowania antywirusowego do komputerów.		
4			

Standardy zabezpieczeń stosowanych:

Zabezpieczenia techniczno-organizacyjne budynku i pomieszczeń:

LP	Zabezpieczenie	Występowanie
1	System alarmowy z monitoringiem i interwencją fizyczną;	1
2	Całodobowy dozór lokalny;	0
3	Drzwi przeciwwłamaniowe z certyfikatem;	1
4	Kraty, rolety przeciwwłamaniowe w oknach;	0
5	System alarmowy;	1
6	Zamki do pomieszczeń z certyfikatem;	1
7	Blokady antywłamaniowe;	0

Zabezpieczenia techniczno-organizacyjne szaf zawierających dokumentację:

LP	Zabezpieczenie	Występowanie
1	Szafy zamykane na klucze;	1
2	Zabezpieczenie szaf zamkami z szyfrem;	1

Zabezpieczenia komputerów:

LP	Zabezpieczenie	Występowanie

1	Program antywirusowy Kaspersky, Microsoft Defender	1
2	Zabezpieczenia użytkowników w postaci loginów i haseł dostępowych.	1
3	Zabezpieczenie przed nieautoryzowanym dostępem do baz danych przez sieć Internet (przed podsłuchiwaniem, przechwytywaniem i atakiem z zewnątrz)	1
4	Odrębne zasilanie sprzętu komputerowego	1
5	Ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na płytach DVD, DVDRW	1
6	Ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na zewnętrznych nośnikach – dyskach twardych	1
7	Ściana przeciwogniowa – składa się z bezpiecznego systemu operacyjnego i filtra pakietów	1
8	Blokowanie wybranych portów	1
9	Zastosowanie Firewoll, którego zadaniem jest uwierzytelnienie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry	1

Procedury i sposoby zagwarantowania realizacji praw osób, których dane są przetwarzane

Procedura zapewnienia prawa dostępu do danych osobowych

1. Każda osoba, której dane której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   a) celu przetwarzania; celu wykorzystania danych;
   b) kategorii i zakresu przetwarzania danych osobowych;
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.

2. Osoba, która chce skorzystać z prawa wskazanego w pkt 1. jest obowiązana do złożenia na piśmie lub w formie elektronicznej z wykorzystaniem profilu zaufanego, podpisu elektronicznego lub platformy ePUAP wniosku o uzyskanie od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, oraz ewentualnego zakresu żądanych informacji.

3. Udzielenie potwierdzenia oraz informacji, o których mowa w pkt 1 i 2. następuje w formie pisemnej informacji. W przypadku złożenia wniosku w formie elektronicznej z zastrzeżeniem wynikającym z pkt 2, udzielenie potwierdzenia oraz informacji, o których mowa w pkt 1 i 2. następuje także w formie elektronicznej.

4. Informacja, o której mowa w pkt 3. jest wydawane w terminie do 30 dni od dnia wpłynięcia wniosku, o którym mowa w pkt 2. tj. informacji na temat wykorzystywania jej danych osobowych (celu, zakresu i sposobu przetwarzania danych oraz źródła uzyskania danych).

5. Na żądanie osoby, której dane osobowe są przetwarzane, jej dane mogą zostać uzupełnione, uaktualnione, sprostowane, względnie czasowo lub w sposób trwały może zostać wstrzymane ich przetwarzanie. O ile dane zostały udostępnione innym Administratorom Danych należy ich bez zbędnej zwłoki powiadomić o dokonanym uaktualnieniu, sprostowaniu lub zastrzeżeniu.

Procedura realizacji uprawnienia: prawo dostępu do danych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa dostępu do swoich danych przetwarzanych przez Administratora.

Każdej osobie fizycznej przysługuje prawo do uzyskania wyczerpujących informacji od Administratora, w postaci potwierdzenia, czy dane są faktycznie przetwarzane przez Administratora.

Prawo dostępu do danych osobowych jest realizowane poprzez wydanie kopii przetwarzanych danych osobie, której dane dotyczą.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba fizyczna, której dane są przetwarzane ma prawo do uzyskania od Administratora następujących informacji:

1) o celach, w jakich przetwarzane są dane osobowe;

2) o kategoriach danych osobowych, które podlegają przetwarzaniu;
3) o odbiorcach lub kategoriach odbiorców;
4) o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania okresu przechowywania danych;
5) o prawie do żądania sprostowania swoich danych osobowych;
6) o prawie do usunięcia lub ograniczenia przetwarzania danych osobowych;
7) o prawie do wniesienia sprzeciwu wobec konkretnego przetwarzania swoich danych;
8) o prawie do wniesienia skargi do organu nadzorczego, na przetwarzanie swoich danych, jeśli są one przetwarzane niezgodnie z obowiązującymi przepisami;
9) w sytuacji, gdy dane osobowe nie zostały zebrane od osoby, której one dotyczą - wszelkich dostępnych informacje o źródle, z którego administrator pozyskał te dane
10) o zautomatyzowanym podejmowaniu decyzji, jeżeli takie administrator realizuje wobec konkretnej osoby fizycznej taki sposób przetwarzania, w tym informacji o profilowaniu (art. 22 ust. 1 i 4 RODO), jak również wszelkie istotne informacje o zasadach podejmowania takich decyzji oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby fizycznej, której przetwarzane dane i decyzje dotyczą.

3. Realizacja uprawnienia dostępu do danych

Osoba fizyczna otrzymuje dostęp do swoich danych osobowych poprzez uzyskanie kopii przetwarzanych danych osobowych. Jeżeli osoba której, dane dotyczą zwraca się o kopię danych drogą elektroniczną to administrator udziela informacji powszechnie stosowaną drogą elektroniczną. Pierwsza kopia i jej przekazanie odbywa się bezpłatnie lecz za wszelkie kolejne kopie, o które zwróci się podmiot danych, Administrator będzie miał prawo pobrać „ opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych" (art. 15 ust. 3 RODO) związanych z jej wytworzeniem (według stawek obowiązujących u Administratora). Umożliwienie wglądu do danych konkretnej osobie fizycznej nie może powodować naruszenia praw innych osób lub też tajemnic prawnie chronionych.
Uzyskując wgląd do swoich danych osoba fizyczna nie może mieć nieuzasadnionego dostępu do danych innych osób fizycznych, lub do danych stanowiących tajemnicę przedsiębiorstwa. W przypadku, gdy przetwarzana jest duża ilość informacji o osobie, która chce skorzystać z prawa dostępu do swoich danych, Administrator kieruje do tej osoby żądanie sprecyzowania do jakich konkretnie danych lub też informacji o czynnościach przetwarzania jej danych chciałaby ona uzyskać dostęp.
<u>Terminy na udzielenie odpowiedzi na żądanie:</u>

1. Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie **miesiąca** od otrzymania tego żądania.
2. Jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań,

administrator może wydłużyć czas udzielenia odpowiedzi o kolejne **2 miesiące,** jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

3. W przypadku, gdy administrator nie zamierza udzielić odpowiedzi oraz podjęcia działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Wzór odpowiedzi na skierowany wniosek:

Na podstawie art. 15 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, Administrator potwierdza, że Pana/Pani dane osobowe są przetwarzane i jednocześnie informuje, że:
1. Celem przetwarzania Pani/Pana danych osobowych jest ……;
2. (Administrator) przetwarza Pani/Pana dane osobowe w zakresie ……. (należy wskazać kategorię danych osobowych);
3. Dane osobowe będą ujawniane ……..... (należy wskazać odbiorcę lub kategorie odbiorców);
4.Dane osobowe będą przechowywane przez okres ……;
5.Przysługuje Panu/Pani prawo do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, a także prawo do wniesienia sprzeciwu oraz skargi do organu nadzorczego;
(Administrator) uzyskał Pani/Pana dane osobowe z ……... (należy wskazać źródło, o ile dane nie zostały pozyskane od osoby, której dotyczą);
6(należy dodać informacje dotyczące zautomatyzowanego podejmowania decyzji, w tym profilowania, o ile znajduje to zastosowanie).

.....
(data, podpis)

Procedura realizacji uprawnienia: prawo do sprostowania danych osobowych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej do sprostowania/uzupełnienia swoich danych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje jednakowe prawo do niezwłocznego

sprostowania/uzupełnienia dotyczących go danych osobowych, które są nieprawidłowe lub nieaktualne. Uwzględniając cele przetwarzania, osoba, której dane dotyczą ma prawo do żądania od Administratora uzupełnienia niekompletnych danych osobowych, poprzez przedstawienie odpowiedniego oświadczenia Administratorowi.

Jeżeli osoba fizyczna zażąda uzupełnienia katalogu dotyczących go danych osobowych o te, które nie są niezbędne Administratorowi do działania, to taki wniosek/oświadczenie woli nie musi zostać pozytywnie rozpatrzony przez Administratora dla osoby, której dane dotyczą.

3. Procedura rozpatrywania żądań o sprostowanie danych osobowych

Komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i dostępnej formie.

Osoba składająca oświadczeni e/wniosek o sprostowani e/uzupełnienie danych osobowych oświadcza, że jest osobą możliwą do zidentyfikowania, na podstawie dobrowolnie podanych danych osobowych, umożliwiających jej jednoznaczną identyfikację.

W przypadku, gdy Administrator nie jest w stanie zidentyfikować osoby składającej oświadczenie/wniosek o sprostowanie/uzupełnienie danych osobowych, ma prawo na podstawie obowiązujących przepisów prawa odmówić rozpatrzenia żądania, uprzednio podejmując wszelkie możliwe środki w celu zidentyfikowania osoby, która z nim wystąpiła.

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) Administratorowi przysługują dwa uprawnienia:

1) pobranie rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań (według stawek obowiązujących u Administratora),
2) odmowa podejmowania działań.

Administrator, w przypadku podjęcia decyzji, o nieuzasadnionym lub nadmiernym charakterze żądania ma obowiązek wykazania takich cech żądania (wniosku) w ewentualnym postępowaniu przed organem nadzorczym.

Administrator jest zobowiązany po dokonaniu sprostowania/ uzupełnienia danych osobowych poinformować wszystkich odbiorców którym ujawniono dane podlegające uzupełnieniu/sprostowaniu o fakcie ich uzupełnienia/sprostowania.

W przypadku braku możliwości wykonania powyższego, lub gdy działanie takie wymagałoby niewspółmiernie dużego wysiłku ze strony Administratora, może on podjąć decyzję o nieudzieleniu stosownej informacji odbiorcom, jednakże ma obowiązek wykazania braku tej możliwości lub niewspółmiernie dużego wysiłku w ewentualnym postępowaniu przed organem nadzorczym.

4. Terminy rozpatrywania żądań o sprostowanie/uzupełnienie danych osobowych.
Na podstawie art. 12 ust. 3 RODO, Administrator podejmuje decyzję o przyjęciu/odrzuceniu oświadczenia/wniosku o sprostowanie/uzupełnienie danych osobowych bez zbędnej zwłoki.

<u>Terminy na udzielenie odpowiedzi na żądanie:</u>

1) Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie **miesiąca** od otrzymania tego żądania;
2) jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne **2 miesiące,** jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

W przypadku, gdy Administrator nie zamierza udzielić odpowiedzi i działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

wniosek o sprostowanie/uzupełnienie danych osobowych

Imię i nazwisko:

……

Adres zamieszkania / adres poczty elektronicznej*:

……

wnioskuję o dokonanie sprostowanie / uzupełnienie moich danych osobowych, w postaci:

……

/należy wymienić o jakie kategorie danych osobowych chodzi oświadczającemu/wnioskującemu/

Podstawa do dokonania sprostowania / uzupełnienia:……. (np. decyzja administracyjna, inny akt prawny, dokument (do wglądu) osobie przyjmującej oświadczenie / wniosek* upoważnionej do tej czynności przez Administratora)

……

/data i czytelny podpis osoby składającej oświadczenie / wniosek */

Procedura realizacji uprawnienia: prawo do usunięcia swoich danych osobowych (*prawo do bycia zapomnianym*)

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa usunięcia swoich danych osobowych („prawo do bycia zapomnianym") przetwarzanych przez Administratora.

1. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje jednakowe prawo żądania usunięcia jego danych osobowych przetwarzanych przez Administratora.

Składa się ono z następujących uprawnień:

1) możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez Administratora danych,
2) możliwości żądania, aby Administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, czy ich replikacje.

Obowiązek poinformowania innych administratorów danych może bvć ograniczony przez:

1) dostępną technologię,
2) koszty,
3) konieczność ograniczenia się Administratora do „rozsądnych działań".

Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

II. Każdemu podmiotowi danych przysługuje jednakowe prawo do „bycia zapomnianym."

Prawo to można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;
3) osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych;
4) dane osobowe były przetwarzane w sposób „niezgodny z prawem";
5) dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator";
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W przypadku wykonania prawa do bycia zapomnianym, Administrator zaprzestaje przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowne oświadczenie/ wniosek, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym:

1) istnieje przepis prawa, który nakazuje przetwarzanie danych osobowych,
2) istnieje sytuacja, w której przetwarzanie jest niezbędne do ustalenia dochodzenia lub obrony roszczeń.

wniosek o usunięcie danych osobowych (prawo do bycia zapomnianym)

Imię i nazwisko:

……

Adres zamieszkania / adres poczty elektronicznej*:

……

wnioskuję* o dokonanie usunięcia moich danych osobowych, w postaci:

……

/należy wymienić o jakie kategorie danych osobowych chodzi oświadczającemu/wnioskującemu/

Podstawa do dokonania usunięcia:

……

(np. decyzja administracyjna, inny akt prawny, dokument (do wglądu), opis sytuacji, mającej podstawę do usunięcia danych osobowych okazane osobie przyjmującej oświadczenie / wniosek* upoważnionej do tej czynności przez Administratora)

……

czytelny podpis osoby składającej wniosek

Procedura realizacji uprawnienia: prawo do przeniesienia swoich danych osobowych

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do przeniesienia swoich danych osobowych przetwarzanych przez Administratora.

1. Prawa osoby fizycznej, której dane są przetwarzane

Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy osoba, której dane dotyczą uprzednio dostarczyła Administratorowi dane jej dotyczące, lub wyraziła zgodę na pozyskanie przez Administratora tych danych, w inny sposób, określony uprzednio odpowiednim oświadczeniem.

Prawo do przenoszenia danych to, w szczególności prawo do:

1) otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi;
2) prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych, o ile jest to technicznie możliwe.

Prawo do przeniesienia danych może zostać wykonane, gdy:

1) przetwarzanie danych odbywa się na podstawie zgody osoby, lub w celu wykonania umowy;
2) przetwarzanie danych odbywa się w sposób zautomatyzowany - prawo do przenoszenia danych obejmuje tylko te dane osobowe, które są przetwarzane przy użyciu systemów informatycznych i nie obejmuje ono tradycyjnych, manualnych papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła Administratorowi. Wykonywanie tego prawa nie może ono niekorzystnie wpływać na praw i wolności innych osób.

Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Wniosek o przeniesienie danych osobowych

Imię i nazwisko:

……

Adres zamieszkania / adres poczty elektronicznej*:

…….

wnioskuję* o dokonanie przeniesienia moich danych osobowych, w postaci:

……

/należy wymienić o jakie kategorie danych osobowych chodzi oświadczającemu/wnioskującemu/

Podstawa do dokonania przeniesienia:

……

(np. decyzja administracyjna, inny akt prawny, dokument (do wglądu), opis sytuacji, mającej podstawę do przeniesienia danych osobowych okazane osobie przyjmującej oświadczenie / wniosek* upoważnionej do tej czynności przez Administratora)

Nazwa podmiotu, do którego należy przenieść dane osobowe wymienione w pkt. 2. :

……

……

/data i czytelny podpis osoby składającej oświadczenie/

Procedura: prawo do sprzeciwu do przetwarzania swoich danych osobowych

1 Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do sprzeciwu do przetwarzania swoich danych osobowych przez Administratora.

1. Prawa osoby fizycznej, której dane są przetwarzane

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, (w tym profilowania na podstawie tych przepisów), tj. sytuacji, w której:

- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
- przetwarzanie jest niezbędne do celów, wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.
- Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, do złożenia sprzeciwu wobec powyższego przetwarzania jej danych osobowych, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
- W sytuacji, gdy Administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym również profilowania, w zakresie, w jakim przetwarzanie jest związane

z takim marketingiem bezpośrednim.

- Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, to Administratorowi nie wolno już przetwarzać tych danych osobowych do takich celów.
- Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
- Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo wnieść bezpłatnie sprzeciw do Administratora, w dowolnym momencie, wobec tego konkretnego przetwarzania, pierwotnego lub dalszego (w tym profilowania), o ile jest ono powiązane z marketingiem bezpośrednim.

Prawo do sprzeciwu musi zostać przez Administratora wyraźnie podane do wiadomości osobie, której dane dotyczą, jak również musi być przedstawione jasno i oddzielnie od wszelkich innych informacji.

2. Szczególne uprawnienia związane z procesami przetwarzania zautomatyzowanego danych - w tym z profilowaniem.

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który:

- odbywa się w sposób automatyczny,
- ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania.

Profilowanie zawsze wymaga poinformowania (w sposób możliwy do zweryfikowania) o nim osób, które są profilowane.

Profilowanie może być wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji Administratora wobec osób, których dane dotyczą.

Jeżeli takie automatyczne podejmowanie decyzji wywołuje skutki prawne wobec osób, których dane dotyczą, lub w podobny istotny sposób wpływa na te osoby, Administrator może mechanizm ten stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

- osoba profilowana wyrazi na to wyraźną zgodę,
- profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
- profilowanie jest dopuszczalne przez szczególne przepisy prawa.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być szczególny przepis prawa.

Jeżeli zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.

Odwołanie zgody wywołuje wyłącznie skutki na przyszłość - oznacza to, że od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już opierać na zgodzie przetwarzania danych.

3. Realizacja prawa do sprzeciwu

Administrator, po wniesieniu sprzeciwu przez osobę, której dane przetwarzał, powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji.

Wykazanie zaistnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, jest obowiązkiem leżącym po stronie Administratora, i ma on obowiązek wykazania powyższego, w ewentualnym postępowaniu przed organem nadzorczym.

Wykorzystanie prawa do sprzeciwu nie prowadzi do automatycznego usunięcia wszystkich danych osobowych przez Administratora. Oznacza ono, że Administrator, z chwilą otrzymania sprzeciwu wobec przetwarzania danych osobowych, zaprzestaje z nich korzystać.

Aby dane osobowe zostały całkowicie usunięte konieczne jest skorzystanie przez osobę, której dane przetwarza Administrator konieczne jest skorzystanie z prawa do usunięcia danych osobowych - prawa do bycia zapomnianym.

Wniosek o wniesienie sprzeciwu o przetwarzanie danych osobowych

Imię i nazwisko:
……

Adres zamieszkania / adres poczty elektronicznej*:
…….

wnioskuję*/ sprzeciwiam się przetwarzaniu moich danych osobowych, w postaci:
……
/należy wymienić o jakie kategorie danych osobowych chodzi oświadczającemu/wnioskującemu/

Podstawa do przyjęcia wniosku o zaprzestanie przetwarzania danych

.....

(np. decyzja administracyjna, inny akt prawny, dokument (do wglądu), opis sytuacji, mającej podstawę do zaprzestania przetwarzania danych osobowych okazane osobie przyjmującej oświadczenie / wniosek* upoważnionej do tej czynności przez Administratora)

Uzasadnienie
sprzeciwu:…….

……
/data i czytelny podpis osoby składającej oświadczenie/

IV. OGÓLNE ZASADY OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH:

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.

2. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.

3. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.

4. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

V. INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Ochrony Danych i Inspektorowi Ochrony Danych.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Danych Osobowych lub Inspektora Ochrony Danych lub upoważnionej przez nich osoby (jeżeli taka jest wyznaczona), osoba stwierdzająca (powiadamiająca) powinna:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
- zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

3. Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administratora Danych Osobowych lub Inspektora Ochrony Danych lub upoważnionej przez nich osoby:

- zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
- wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- Administrator Danych Osobowych i Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.

4. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Danych Osobowych i Inspektor Ochrony Danych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

VI. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Odpowiedzialny za przeprowadzenie kontroli oraz badanie stanu zabezpieczeń ochrony danych jest Administrator Danych Osobowych.

2. Odpowiedzialny za przeprowadzenie kontroli / audytów oraz badanie stanu zabezpieczeń ochrony danych jest Inspektor Ochrony Danych.

3. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25 - 401 Kielce sprawują Administrator Danych Osobowych oraz Inspektor Ochrony Danych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.

4. Inspektor Ochrony Danych dokonuje czynności kontrolnych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami rozporządzenia o ochronie danych osobowych.

5. Sprawdzenia dokonywane jest przez Inspektora Ochrony Danych dla Administratora Danych, bądź dla Urzędu Ochrony Danych Osobowych, gdy ten na podstawie przysługujących mu kompetencji zwróci się o to do Administratora Danych lub Inspektora Ochrony Danych.

6. IOD przeprowadza sprawdzenie w trybie:

   - Sprawdzenia planowego - według opracowanego planu sprawdzeń;

   - Sprawdzenia doraźnego - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, niezwłocznie po powzięciu przez IOD takich informacji;

   - Sprawdzenia w przypadku zwrócenia się o to przez Urząd Ochrony Danych Osobowych.

7. Inspektor Ochrony Danych opracowuje plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

8. W toku sprawdzenia IOD dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

9. Po zakończeniu sprawdzenia, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.

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

11. Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych stanowi załącznik do Polityki Bezpieczeństwa

12. Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w pkt 8 stanowi załącznik do Polityki Bezpieczeństwa

Procedura zapewnienia prawa do uzyskania kopii danych osobowych

1. Każda osoba, której dane dotyczą, ma prawo żądać wydania kopii danych osobowych podlegających przetwarzaniu.

2. Osoba, która chce skorzystać z prawa wskazanego w pkt 1. jest obowiązana do złożenia na piśmie lub w formie elektronicznej z wykorzystaniem profilu zaufanego, podpisu elektronicznego lub platformy ePUAP wniosku o uzyskanie od administratora kopii danych osobowych podlegających przetwarzaniu.

3. Wydanie kopii danych osobowych podlegających przetwarzaniu polega na wykonaniu kserokopii odpowiedniego dokumentu zawierającego dane osobowe podlegające przetworzeniu bądź wydaniu wypisu zawierającego wykaz przedmiotowych danych.

4. W przypadku złożenia wniosku w formie elektronicznej z zastrzeżeniem wynikającym z pkt 2, wydanie kopii danych osobowych podlegających przetwarzaniu następuje także w formie elektronicznej.

5. Wybór jednej z form wskazanych w pkt 3. dokonywany jest każdorazowo przez pracownika organu, z uwzględnieniem nakładu pracy oraz kosztów wydania kopii danych.

6. Wydanie kopii danych osobowych podlegających przetwarzaniu następuje w terminie do 7 dni od dnia wpłynięcia wniosku, o którym mowa w pkt 2.

Zasady powoływania i funkcjonowania Inspektora Ochrony Danych Osobowych

1. Inspektor Ochrony Danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań przewidzianych w przepisach prawa.
2. W przypadku powierzenia funkcji Inspektora Ochrony Danych Osobie dotychczas zatrudnionej w organie, zawierana jest z nim dodatkowa umowa o świadczenie usług.
3. W przypadku powierzenia funkcji inspektora ochrony danych osobie dotychczas niezatrudnionej w organie, zawierana jest z nim umowa o pracę lub umowa o świadczenie usług.
4. Inspektor ochrony danych bezpośrednio podlega bezpośrednio kierownikowi/dyrektorowi organu UODO.
5. W związku z wykonywanymi zadaniami z zakresu ochrony danych osobowych, Inspektor Ochrony Danych osobowych nie może być odwoływany ani karany.
6. Do zadań inspektora ochrony danych należy w szczególności:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3.Rejestr operacji przetwarzania danych osobowych W Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25 - 401 Kielce.

Dane kontaktowe		
	Dane	Uwagi
Imię i nazwisko / nazwa administratora danych	Pan Tomasz Kozieł - Dyrektor Zespołu Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach z siedzibą ul. Warszawska 96, 25 – 401 Kielce	
Kontakt do administratora danych	Zespół Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25 - 401 Kielce, tel: 41-367-67-90,fax: 41-367-69-33, e-mail: szkola@zsi.kielce.pl	
Imię i nazwisko / nazwa inspektora ochrony danych	Anna Rubinkiewicz	
Kontakt do inspektora ochrony danych	Tel: 602-779-754 email. abcrodo@op.pl	
Cele przetwarzania danych osobowych		
	Opis celów	Uwagi
Wynikające z ustawy o systemie oświaty USTAWA z dnia 7 września 1991 r. o systemie oświaty		
Wynikające z Kodeksu Pracy USTAWA z dnia 26 czerwca 1974 r. Kodeks pracy		
Wynikające z USTAWA z dnia 26 stycznia 1982 r. Karta Nauczyciela		
Wynikające z Kodeksu cywilnego Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny.		
Wynikające z ustawy o pomocy państwa w wychowywaniu dzieci		
Wynikające z ustawy o przeciwdziałaniu przemocy w rodzinie		
Przetwarzane dane osobowe		
	Opis kategorii danych	Przewidywany termin usunięcia danych
Kategorie przetwarzanych	imię i nazwisko dziecka	Bliżej nie określony.

danych osobowych dzieci / rodziców/ opiekunów prawnych/ nauczycieli / pracowników administracji i obsługi / innych pracowników	adres zamieszkania dziecka / rodziców PESEL, NIP numer legitymacji szkolnej płeć numer telefonu adresy poczty elektronicznej wizerunek dziecka wizerunek nauczyciela wizerunek rodzica (w przypadku imprez szkolnych / publicznych) imiona rodziców, opiekunów nazwisko rodowe matki, numer i seria dowodu osobistego wykształcenie zawód numer i seria dowodu osobistego, adresy poczty elektronicznej rodzica / opiekuna numer telefonu rodzica, stopień awansu zawodowego w przypadku nauczycieli, imiona i daty urodzenia współmałżonka i dzieci nauczycieli (cel - komisje socjalne)	
Szczególne kategorie przetwarzanych danych osobowych	• stan zdrowia dziecka (orzeczenia lekarskie) • pochodzenie • wyznanie religijne	
	Opis kategorii osób	Uwagi
Kategorie osób, których dane dotyczą	Uczniowie, Nauczyciele Pracownicy administracji Pracownicy obsługi Rodzice / opiekunowie prawni	
Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione		– dane przekazywane do dalszego prowadzenia procesu nauczania i wychowania,

3. Rejestr czynności przetwarzania danych osobowych (załącznik)

5. Polityka monitorowania i reagowania na naruszenia ochrony danych w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedzibą ul. Warszawska 96, 25 - 401 Kielce

Polityka monitorowania ochrony danych

1. Bieżący monitoring przestrzegania niniejszej polityki, stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń dokonywany jest przez Inspektora Ochrony Danych.

2. Inspektor Ochrony Danych przynajmniej raz na 6 miesięcy dokonuje audytu polityki bezpieczeństwa w zakresie stosowania przewidzianych nią procedur oraz adekwatności stosowanych środków zabezpieczeń. Po przeprowadzonym audycie inspektor zobowiązany jest opracować pisemny raport dla administratora danych. Raport powinien zawierać ocenę oraz propozycje w zakresie ewentualnych modyfikacji stosowanych procedur oraz środków zabezpieczeń.

3. Na podstawie raportu wskazanego w pkt 2. administrator danych określa kierunki ewentualnych zmian oraz określa termin na ich wprowadzenie.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5. Rejestr incydentów.

LP	Data zdarzenia	
1.	imię i nazwisko osoby zgłaszającej incydent	
2.	imię i nazwisko osoby przyjmującej zgłoszenie incydentu	
3.	data i godzinę przyjęcia zgłoszenia incydentu	
4.	określenie czasu i miejsca incydentu	
5.	opis zgłoszonego incydentu oraz okoliczności towarzyszące	
6.	przyczyny wystąpienia naruszenia	
7.	opis podjętych działań naprawczych	
8.	wyniki przeprowadzonego badania wyjaśniającego	
9.	ocena skuteczności przeprowadzonego postępowania naprawczego	

10.	podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych	

6. Procedury zarządzania użytkownikami i dostępem do danych (załącznik)

a) Wykaz pomieszczeń w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* w Kielcach z siedzibą ul. Warszawska 96, 25 - 401 Kielce tworzących obszar, w którym przetwarzane są dane osobowe.

(załącznik nr 1)

Lp.	Nazwa pomieszczenia	Lokalizacja	Rodzaj Zabezpieczenia	Typ danych w pomieszczeniu
Budynek piętrowy usytuowany przy ul. Warszawskiej 96, 25- 401 Kielce, z parkingiem przed budynkiem dla pracowników / gości, teren ogrodzony, zamykany na klucz, wyposażony w monitoring dla zachowania bezpieczeństwa.				
1.	Sekretariat/ obsługa kadrowa		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenia zamykane na klucz, 3. Wszystkie klucze zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.
2.	Gabinety Dyrektora / Wicedyrektorów		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione. Dane dostępne i przetwarzane na bieżąco. Dane przechowywane w systemie zarządzania Szkołą oraz w wersji papierowej
3.	Sale lekcyjne z zapleczami		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych.	Dane zwykłe, dane szczególnie chronione. Dane dostępne i przetwarzane na bieżąco tylko podczas zajęć lekcyjnych

			4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	
4.	Pokój Kierownika Szkolenia Praktycznego		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.
5.	Pokój nauczycielski		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.
6.	Pokój pedagoga szkolnego		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.
7.	Biblioteka		1.Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2.Pomieszczenie zamykane na klucz, 3.Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4.Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane dostępne i przetwarzane na bieżąco.
8.	Pokoje działu księgowości		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane	Dane zwykłe, dane szczególnie chronione dane dostępne i przetwarzane na bieżąco.

			na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 4. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	
9.	Archiwum szkolne		1. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 2. Pomieszczenie zamykane na klucz, 3. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych.	
10.	Serwerownia			
11.	Pokój Kierownika gospodarczego		5. Zabezpieczenia opisane powyżej w punkcie Standardy zabezpieczeń stosowanych. 6. Pomieszczenie zamykane na klucz, 7. Wszystkie klucze od szaf zamknięte w innym pomieszczeniu w skrzynce z kluczem. Dostęp do pomieszczenia tylko dla pracowników upoważnionych. 8. Komputery zabezpieczone loginem i hasłem, programem antywirusowym.	Dane zwykłe, dane dostępne i przetwarzane na bieżąco.

b) Ewidencja osób upoważnionych do przetwarzania danych osobowych w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedzibą ul. Warszawska 96, 25 - 401 Kielce

(załącznik nr 2)

Lp.	Nazwisko i Imię	Stanowisko / funkcja	Rodzaj Uprawnienia / Cel przetwarzania	Typ powierzonych danych.	Okres powierzenia
1.		ADO Dyrektor	Uprawnienie do przetwarzania danych osobowych pracowników zatrudnionych wg umowy. Uprawnienie pełne do przetwarzania danych uczniów, rodziców, podmiotów przetwarzających.	Uprawnienie pełne do danych zwykłych i szczególnie chronionych	Czas trwania umowy cywilno-prawnej o zatrudnieniu.
2.		Wicedyrektor	Uprawnienie do przetwarzania danych osobowych pracowników zatrudnionych wg umowy.	Uprawnienie do danych zwykłych i szczególnie	Czas trwania umowy cywilno-prawnej o

			Uprawnienie pełne do przetwarzania danych uczniów, rodziców, podmiotów przetwarzających.	chronionych	zatrudnieniu.
3.		Księgowa	Uprawnienie do przetwarzania danych osobowych pracowników zatrudnionych wg umowy. Uprawnienie pełne do przetwarzania danych uczniów, rodziców, podmiotów przetwarzających.	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy cywilno-prawnej o zatrudnieniu.
4.		Kadrowa	Uprawnienie do przetwarzania danych zwykłych pracowników	Uprawnienie do danych zwykłych	Czas trwania umowy cywilno-prawnej o zatrudnieniu.
		Nauczyciel	Uprawnienie do przetwarzania danych zwykłych , ew. szczególnie chronionych uczniów, danych zwykłych rodziców.	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy cywilno-prawnej o zatrudnieniu.
5.		Pedagog szkolny	Uprawnienie do przetwarzania danych zwykłych , ew. szczególnie chronionych uczniów, danych zwykłych rodziców.	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy cywilno-prawnej o zatrudnieniu.
6.		Kierownik Szkolenia Praktycznego	Uprawnienie do przetwarzania danych zwykłych , ew. szczególnie chronionych uczniów, danych zwykłych rodziców.	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy cywilno-prawnej o zatrudnieniu.
7.		Kierownik gospodarczy	Uprawnienie do przetwarzania danych zwykłych pracowników	Uprawnienie do danych zwykłych	Czas trwania umowy cywilno-prawnej o zatrudnieniu.
8.					

c) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Lp.	Nazwa Zbioru	Przechowywanie i zabezpieczenie	Zawartość Zbioru	Dostęp do Zbioru	Okres przechowywania
1.	*Kartoteki danych uczniów Zespołu Szkół Informatycznych im. gen. Józefa Hauke Bosaka w Kielcach. Wersja papierowa*	Pomieszczenie sekretariatu zamykane na klucz, szafy aktowe zamykane z dokumentacją.	Dane osobowe uczniów i rodziców Uprawnienie pełne do przetwarzania danych.	Uprawnienie pełne do danych zwykłych i szczególnie chronionych dla ADO, i osób upoważnionych. Uprawnienie pełne do danych zwykłych dla sekretarki.	Okres nie dłuższy, niż niezbędny do celów przetwarzania, i archiwizacji dokumentów absolwentów.
2.	*Kartoteki danych uczniów Zespołu Szkół Informatycznych im. gen. Józefa Hauke Bosaka w Kielcach . Wersja elektroniczna*	Pomieszczenie sekretariatu zamykane na klucz. System komputerowy z oprogramowaniem antywirusowym. Zabezpieczenia systemowe loginy i hasła dla użytkowników uprawnionych. Program zarządzania Szkołą – dostęp dla osób uprawnionych.	Dane osobowe uczniów i rodziców Uprawnienie pełne do przetwarzania danych.	Uprawnienie pełne do danych zwykłych i szczególnie chronionych dla ADO, i osób upoważnionych. Uprawnienie pełne do danych zwykłych dla sekretarki. Program zarządzający Szkołą dostęp dla uprawnionych pracowników poprzez zabezpieczony komputer.	Okres nie dłuższy, niż niezbędny do celów przetwarzania, i archiwizacji dokumentów absolwentów i pracowników.
3.	*Kartoteki danych, umowy z pracownikami Zespołu Szkół Informatycznych im. gen. Józefa Hauke Bosaka w Kielcach i Podmiotami przetwarzającymi. Wersja papierowa.*	Pomieszczenie sekretariatu, księgowości zamykane na klucz.	Dane osobowe zwykłe pracowników zatrudnionych wg umowy. Dane Podmiotów przetwarzających. Dane niezbędne do realizacji zawartych umów.	Uprawnienie pełne do danych zwykłych i niezbędnych do realizacji i egzekwowania obowiązków wynikających z umowy dla Administratora Danych Osobowych.	Czas trwania umowy cywilno-prawnej o zatrudnieniu / umowy o współpracy / świadczeniu usług.
4.	*Kartoteki danych, umowy z pracownikami Zespołu Szkół Informatycznych im. gen. Józefa Hauke Bosaka w Kielcach i Podmiotami przetwarzającymi. Wersja elektroniczna.*	Pomieszczenie sekretariatu, księgowości zamykane na klucz. System komputerowy z oprogramowaniem antywirusowym. Zabezpieczenia systemowe loginy i hasła dla użytkowników uprawnionych. Program zarządzania Szkołą – dostęp dla osób uprawnionych.	Dane osobowe zwykłe pracowników zatrudnionych wg umowy. Dane Podmiotów przetwarzających. Dane niezbędne do realizacji zawartych umów.	Uprawnienie pełne do danych zwykłych i niezbędnych do realizacji i egzekwowania obowiązków wynikających z umowy dla Administratora Danych Osobowych.	Czas trwania umowy cywilno-prawnej o zatrudnieniu / umowy o współpracy / świadczeniu usług.

Programy przetwarzające dane osobowe dotyczące uczniów:

- System Informacji Oświatowej
- Sekretariat Optivum
- Nober Optivum
- Mol Optivum
- Dziennik elektroniczny (wg zawartej umowy uzytkowania)

Programy przetwarzające dane osobowe dotyczące pracowników:

- System Informacji Oświatowej
- Arkusz Optivum
- Plan Lekcji Optivum
- Synergia Librus
- Księgowość Optivum
- Płace Optivum
- Płatnik
- Elektroniczna Bankowość Banku Śląskiego

Przepływ danych – Dziennik elektroniczny – Program docelowy – Świadectwo Optivum

d) Wzór oświadczenia o zachowaniu poufności.

(załącznik nr 3)

e) Wzory upoważnień otrzymanych od Uczniów / Rodziców / Opiekunów Prawnych / Pracowników. (załącznik)

f) Procedura wyboru i weryfikacji podmiotu przetwarzającego dane.

1) Każdy podmiot zewnętrzny przetwarzający dane zgromadzone przez tut. organ ma obowiązek zapewnić adekwatne środki i standardy zabezpieczenia przekazanych mu danych.
2) Warunkiem przekazania podmiotowi zewnętrznemu danych zgromadzonych przez tut. organ jest zawarcie z podmiotem zewnętrznym umowy o powierzenie danych osobowych
3) Wzór umowy o powierzenie danych osobowych stanowi załącznik nr 4 do niniejszej polityki.

g) **Wykaz podmiotów przetwarzających dane na zlecenie Administratora danych w Zespół Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25-401 Kielce**

(załącznik nr 5)

Lp.	Nazwisko i Imię / Firma	Rodzaj powiązania / umowy z administratorem	Rodzaj Uprawnienia / Cel przetwarzania	Typ powierzonych danych.	Okres powierzenia	Zastosowane środki bezpieczeństwa ochrony danych osobowych
1.		Umowa o wykonywaniu usług –	Umowa powierzenia danych	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy	Dane przesyłane przez upoważnione osoby – bezpośrednio do placówki przetwarzającej i ADO.

2.		Umowa o wykonywaniu usług związanych z dostawą i serwisem systemu zarządzania Szkołą	Umowa powierzenia danych	Uprawnienie do danych zwykłych i szczególnie chronionych	Czas trwania umowy	Dane przesyłane przez upoważnione osoby – bezpośrednio do placówki przetwarzającej i ADO. Pełne zabezpieczenia systemów informatycznych.

h) **Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych w Zespole Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25-401 Kielce**

Środek ochrony fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).	TAK	
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą krat, rolet lub folii antywłamaniowej.**	NIE	
3. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**	TAK	
4. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych objęte są **systemem kontroli dostępu.**	TAK	
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**	TAK	
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**	TAK	
7. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**	TAK	
8. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**	TAK	
9. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**	TAK	
10. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**	TAK	

11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie**.	NIE	
12. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**	TAK	
13. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**	TAK	

ŚRODKI TECHNICZNE

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	**Zastosowano (TAK / NIE)**	**Uwagi**
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	TAK	
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	TAK	
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	TAK	
Użyto system Firewall do ochrony dostępu do sieci komputerowej.	TAK	

ŚRODKI ORGANIZACYJNE

Środek organizacyjny	**Zastosowano (TAK / NIE)**	**Uwagi**
Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	TAK	
Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	TAK	
Powołano Administratora Bezpieczeństwa Informacji	TAK	
Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych	TAK	

Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	TAK	
Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	TAK	
Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	TAK	
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	TAK	
Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	TAK	
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	TAK	

\

……..

miejscowość, data

SPRAWOZDANIE

ZE SPRAWDZENIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

z przepisami o ochronie danych osobowych

1. Administrator Danych: Zespół Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25-401 Kielce

2. Inspektor Ochrony Danych: Anna Rubinkiewicz

3. Wykaz czynności podjętych w toku sprawdzenia:

   ……
   ……
   ……

4. Data rozpoczęcia sprawdzenia:

   …….....

5. Data zakończenia sprawdzenia:

   ……

6. Przedmiot i zakres sprawdzenia:

   ……
   ……
   ……

7. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych: …….

   ……
   ……
   ……

8. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

   ……
   ……
   ……

   Załączniki:……

……
Podpis IOD

……
miejscowość, data

PROTOKÓŁ
Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*
w zakresie ochrony danych osobowych

Nazwa kontrolowanej jednostki organizacyjnej: **Zespół Szkół Informatycznych *im. gen. Józefa Hauke Bosaka* z siedziba ul. Warszawska 96, 25-401 Kielce**

1. Zbiory danych osobowych, których przetwarzanie podlega kontroli:

   ……..
   .....

2. Data wykonania czynności kontrolnych:……..

3. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne:

   ……..

4. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej

   ……..…..……

6. Ustalenia dokonane w trakcie czynności kontrolnych:……

   ……
   ……
   ……
   ……

   Wnioski i zalecenia pokontrolne:

   ……
   ……
   ……

(data i podpis osoby wykonującej czynności kontrolne)

……
(data i podpis Dyrektora Zespołu Szkół Informatycznych w Kielcach)

Otrzymują:
1 x Dyrektor Zespołu Szkół Informatycznych w Kielcach
1 x Inspektor Ochrony Danych

* niepotrzebne skreślić

Administrator Danych Osobowych

……
Podpis