POLITYKA OCHRONY DANYCH OSOBOWYCH

Samorządowa Administracja Placówek Oświatowych w Poczesnej

SPIS TREŚCI

<u>Załączniki:</u>

1. *Wykaz pomieszczeń, w których przetwarzane są dane osobowe (obszar).*
2. *Rejestr upoważnień.*
3. *Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych.*
4. *Wykaz udostępnień danych osobowych.*
5. *Rejestr zbiorów danych osobowych.*
6. *Rejestr incydentów i zagrożeń.*
7. *Rejestr czynności przetwarzania.*
8. *Zalecenia IODO.*

Rozdział 1.
Postanowienia ogólne. Podstawy prawne. Słownik pojęć. Cel. Zakres.

§ 1.

Podstawa prawna :

- Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U.2018.1000 z dnia 2018.05.24)
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)(Dz.Urz.UE L119 z 4 maja 2016 r.).

§ 2.
Słownik pojęć

1. Administrator Danych Osobowych (ADO) -organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych. W tym przypadku Administratorem Danych Osobowych jest Samorządowa Administracja Placówek Oświatowych w Poczesnej.
2. Inspektor Ochrony Danych Osobowych (IODO) - osoba fizyczna lub prawna powoła na przez Administratora Danych Osobowych, zajmująca się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem rejestru zbiorów danych przetwarzanych przez administratora danych.
3. Baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe.
4. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której 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.
5. Droga elektroniczna – poczta elektroniczna lub elektroniczna skrzynka podawcza, o której mowa w art. 3 pkt 7 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. 2017 r., poz. 570).
6. Działanie korygujące -działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji.
7. Działanie zapobiegawcze -działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności/incydentu lub innej potencjalnej sytuacji niepożądanej.
8. Hasło – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

9. Identyfikator Użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
10. Incydent -pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego i zagrażają bezpieczeństwu informacji; naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
11. Kontrola (Audyt) -systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań polityk i procedur.
12. Niezgodność -niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
13. Nośniki danych – przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania transmisji. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych.
14. Odbiorca danych – każdy, komu udostępniane są dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela administratora danych mającego siedzibę w państwie trzecim, przetwarzającego dane przy wykorzystaniu środków technicznych znajdujących się na terytorium RP, podmiotu który przetwarza dane na podstawie umowy powierzenia zawartej z administratorem, a także organów państwowych i organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem (art. 7 pkt 6 ustawy).
15. Pracownik – osoba fizyczna świadcząca na rzecz ADO pracę na podstawie stosunku pracy.
16. Przetwarzane danych – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym.
17. System informatyczny (system IT) -zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
18. System tradycyjny -zespół procedur organizacyjnych, wyposażenia i środków trwałych związanych z mechanicznym przetwarzaniem informacji zawierających dane osobowe na nośnikach papierowych.
19. Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
20. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
21. Użytkownik – pracownik lub współpracownik ADO oraz każda inna osoba, która uzyskała upoważnienie do przetwarzania danych osobowych w systemach, a także osoba upoważniona przez ADO, z którym została podpisana umowa powierzenia przetwarzania danych osobowych.

§ 3.
Cel i zakres.

1. Polityka Ochrony Danych Osobowych – zwana dalej Polityką Ochrony jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych u ADO.
2. Polityka Ochrony została opracowana i wdrożona w celu uzyskania standardu przetwarzania informacji zawierających dane osobowe zgodnego z wymaganiami określonymi w przepisach prawa, w szczególności danych osobowych przetwarzanych w celu służącym realizacji zadań jednostki oświaty.
3. Niniejszy dokument musi zostać udostępniony każdej osobie mającej dostęp do danych osobowych przetwarzanych u ADO.

§ 4.

1. Polityka Ochrony określa w szczególności:
   - prawa i obowiązki osób przetwarzających dane osobowe w związku z działalnością ADO;
   - sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych, w tym podstawowe warunki jakim powinny odpowiadać urządzenia z wykorzystaniem których dane są przetwarzane;
   - zasady prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych,
   - instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych;
2. Zastosowane zabezpieczenia mają zapewnić:

- poufność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom;
- integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalność danych -rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
- integralność systemu -rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej;
- dostępność informacji -rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
- zarządzanie ryzykiem -rozumiane jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.

Rozdział 2.

Administrator Danych Osobowych. Inspektor Ochrony Danych Osobowych.

§ 5.

1. Administrator Danych Osobowych podejmuje decyzje w zakresie realizacji celów i zapewnienia środków zapewniających bezpieczeństwo przy przetwarzaniu danych osobowych, zgodnie z wymogami i zaleceniami wynikającymi z przepisów prawa, w celu ochrony interesów osób, których dane dotyczą.
2. Administrator Danych Osobowych pełni funkcję kontrolną w zakresie poprawnego przetwarzania danych osobowych oraz nadzoruje przestrzeganie ustalonych zasad zawartych w Polityce Ochrony.
3. Administrator Danych Osobowych jest zobowiązany do zgłoszenia Prezesowi Urzędu Ochrony Danych Osobowych powołania (lub odwołania) Inspektora Ochrony Danych Osobowych (IODO).
4. Zadania Administratora Danych Osobowych obejmują :

a) wypełnianie obowiązku informacyjnego przy zbieraniu danych osobowych w tym udzielanie informacji o celu i zakresie przetwarzanych danych osobowych;
b) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza;
c) obowiązek uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;
d) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
e) nadawanie, zmianę i anulowanie upoważnień do przetwarzania danych osobowych;
f) obowiązek kontrolowania jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane;
g) obowiązek prowadzenia wykazu osób upoważnionych do przetwarzania danych osobowych.

§ 6.

1. Inspektor Ochrony Danych Osobowych (IODO) jest powoływany przez ADO drogą pisemnego upoważnienia.
2. Do kompetencji IODO należy w szczególności:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie sprawozdań dla ADO;
- nadzorowanie przestrzegania zasad ochrony danych osobowych tj. środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, ze szczególnym uwzględnieniem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w tym nadzór nad obiegiem oraz przechowywaniem materiałów i dokumentów zawierających dane osobowe w zakresie dotyczącym systemu IT;
- nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych, środki ich ochrony oraz przestrzegania zasad w niej określonych;
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

- wnioskowanie i opiniowanie wniosków do ADO o nadanie, zmianę lub cofnięcie uprawnień dostępu do danych osobowych oraz pozostałych wniosków dotyczących bezpieczeństwa informacji, w tym danych osobowych, a także nadzór w zakresie realizacji tych wniosków;
- nadzór nad fizycznym zabezpieczeniem pomieszczeń we współpracy z ADO, w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób;
- zapewnienie przeciwdziałania incydentom oraz prowadzenie rejestru incydentów i zagrożeń;
- szkolenie osób upoważnionych do przetwarzania danych osobowych w zakresie przepisów o ochronie danych osobowych oraz zapewnienie bieżącej edukacji Użytkowników w zakresie polityki bezpieczeństwa, w tym wnioskowanie do ADO o organizację tych szkoleń.

§ 7.

1. IODO prowadzi jawny rejestr zbiorów danych osobowych przetwarzanych na potrzeby realizacji celów i zadań ADO oraz wykaz zbiorów zawierający strukturę zbiorów, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi wraz z programami zastosowanymi do ich przetwarzania. Rejestr prowadzony jest w oparciu o wzór określony w Załączniku nr 5 do Polityki Ochrony.
2. W ramach nadzoru nad przetwarzaniem danych, IODO sprawdza w szczególności cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia danych osobowych, w tym zabezpieczenia urządzeń mobilnych wykorzystywanych w działalności ADO. IODO jest również zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym oraz tradycyjnym z uwzględnieniem specyfiki pracy wiążącej się z koniecznością przetwarzania danych osobowych poza siedzibą ADO z wykorzystaniem urządzeń mobilnych.
3. Ponadto IODO jest odpowiedzialny za prowadzenie i aktualizację wykazu budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania wykazu udostępnień danych osobowych innym podmiotom wykazu podmiotów, którym powierzono dane osobowe do przetwarzania oraz wykazu udostępnień danych osobowych osobom, których dane dotyczą.

Rozdział 3.
Zasady przetwarzania danych osobowych. Powierzenie. Udostępnianie. Obowiązek informacyjny. Zgoda. Zabezpieczenia. Sprawdzenia. Odpowiedzialność.

§ 8.

1. Zasady przetwarzania danych osobowych:

a) dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. ADO może żądać podania jedynie tych danych, które są niezbędne do realizacji jej celów i zadań;

b) zakres danych osobowych przetwarzanych przez pracownika nie może być szerszy niż powierzony do przetwarzania w związku z wykonywanymi przez niego obowiązkami;
c) po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą, zniszczone lub, w przypadku powierzenia, zwrócone podmiotowi, który dane powierzył.

2. Zasady ochrony danych osobowych mają zastosowanie do:

a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów przetwarzania informacji zawierających dane osobowe, w tym systemów IT;
b) informacji będących własnością ADO oraz przetwarzanych przez niego w związku z prowadzoną działalnością;
c) wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
d) wszystkich osób świadczących pracę lub wykonujących czynności na rzecz ADO mających dostęp do informacji podlegających ochronie.

§ 9.

Przetwarzanie danych osobowych odbywa się z wykorzystaniem dokumentów, materiałów, przesyłek analogowych (nieelektronicznych), wniosków, pism, akt osobowych pracowników, dokumentów finansowo-księgowych, podań itp. oraz danych zawartych na nośnikach elektronicznych, magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych, a także danych przetwarzanych w systemie kadrowo-płacowym, programie Vulcan, SIO, systemie do obsługi dokumentów ubezpieczeniowych i wymianie informacji z ZUS, systemie teleinformatycznym administracji.

§ 10.

1. Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia w siedzibie ADO. Opis obszaru następuje według wzoru określonego w Załączniky nr 1 do niniejszej Polityki Ochrony.
2. Dane osobowe umieszczone są w pomieszczeniach, gdzie kontrolowany jest ruch osobowy i materiałowy, do których dostęp posiadają pracownicy oraz współpracownicy ADO oraz pozostałe osoby przebywające w tej strefie w związku z wykonywanymi obowiązkami lub czynnościami (umowy powierzenia).

§ 11.

Wszystkie osoby, które posiadają dostęp do danych osobowych w obszarze wymienionym w § 10 muszą posiadać upoważnienie do przetwarzania danych ze wskazaniem zakresu dostępu do tych danych.

§ 12.

1. Uprawnienia do przetwarzania danych osobowych w programach związanych z działalnością jednostki oświaty nadawane są zgodnie z właściwą procedurą określoną

przez Dyrektora. Wybrani pracownicy posiadają uprawnienia do obsługi programu. Uprawnienia ważne są do dnia odwołania lub do chwili ustania zatrudnienia uprawnionego pracownika.

§ 13.

1. Ochrona dotyczy w szczególności:
a) danych osobowych gromadzonych i przetwarzanych w związku z działalnością ADO , w tym danych osobowych uczniów/dzieci, rodziców/opiekunów prawnych.
b) danych osobowych pracowników, w tym danych osobowych i treści zawieranych umów o pracę,
c) danych osobowych kandydatów do pracy zbieranych na etapie rekrutacji;
d) danych osobowych zawartych w dokumentach finansowo-księgowych ;
e) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł do programów, oraz haseł dostępu do komputerów dla każdego użytkownika,
f) danych osobowych zawartych w rejestrze osób dopuszczonych do przetwarzania danych osobowych;
g) danych osobowych zawartych w pozostałych dokumentach wytwarzanych w związku z działalnością ADO.
2. Katalog zbiorów przetwarzanych danych osobowych może ulec rozszerzeniu, w zależności od zakresu bieżącej działalności ADO.

§ 14.

1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy, współpracownicy lub pracownicy podmiotów współpracujących lub świadczących usługi na rzecz ADO w zakresie adekwatnym do celu powierzenia.
2. Upoważnienie do przetwarzania danych osobowych następuje w formie pisemnej wraz z określeniem zbioru danych oraz poziomem dostępu do tych danych.
3. Inspektor Danych Osobowych prowadzi rejestr upoważnień według wzoru stanowiącego Załącznik nr 2 do niniejszej Polityki Ochrony.
4. Powierzenie przetwarzania danych osobowych innym podmiotom niż określone w ust. 1 następuje na podstawie umowy powierzenia zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej (oświadczenie złożone drogą elektroniczną lub zapisane na elektronicznym nośniku informacji).
5. Umowa powierzenia danych osobowych określa przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy (administratora i procesora).
6. Podmiot, z którym zostaje zawarta umowa powierzenia jest zobowiązany do wdrożenia środków organizacyjnych i technicznych odpowiednich do ryzyk przetwarzania powierzonych danych, prowadzenia rejestru czynności przetwarzania, zgłaszania naruszeń ochrony danych do organu nadzorczego.
7. IODO prowadzi wykaz podmiotów, którym powierzono przetwarzanie danych osobowych, według wzoru stanowiącego Załącznik nr 3 do Polityki Ochrony.

§ 15.

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności.
2. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych.
3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.
4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.
5. Udostępnienie danych osobowych osobom, których dane dotyczą odbywa się na wniosek tych osób. Udostępnienie poprzedza weryfikację tej osoby.
6. ADO prowadzi wykaz udostępnień wg wzoru stanowiącego Załącznik nr 4 do Polityki Ochrony.

§ 16.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany poinformować tę osobę o:
    a) adresie swojej siedziby i pełnej nazwie;
    b) celu i zakresie zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
    c) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej i konsekwencjach niepodania danych;
    d) wyznaczonym Inspektorze Ochrony Danych Osobowych – jego danych osobowych oraz danych kontaktowych (adres e-mail);
    e) prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywać się będzie przetwarzanie danych;
    f) okresie, przez który dane osobowe będą przechowywane lub o kryteriach tego okresu;
    g) profilowaniu danych;
    h) prawach osoby, której dane dotyczą tj. prawie do usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).
2. W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, ADO jest zobowiązany poinformować tę osobę źródle pozyskania danych oraz uprawnieniach w tym przypadku z przepisów prawa.

3. Obowiązek poinformowania wymieniony w ust. 1 niniejszego paragrafu powinien być wykonany w momencie zbierania danych z wyjątkiem sytuacji, w której przepis innej ustawy zezwala na przetwarzanie danych osobowych lub osoba, której dane dotyczą, posiada już informacje.
4. Obowiązek poinformowania wymieniony w ust. 2 niniejszego paragrafu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie.

§ 17.

1. Zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
2. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana ani wynikać z oświadczenia woli o innej treści, tzn. zgoda nie może być zawarta np. w regulaminie, którego zaakceptowanie wiąże się ze zgodą na warunki w nim zawarte.
3. W przypadku pozyskania zgody w formie innej niż pisemna, na ADO ciąży obowiązek udowodnienia, że została ona pozyskana, a nie dorozumiana.
4. Zgoda na przetwarzanie danych osobowych powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, należy pozyskać odrębną zgodę na każdy cel.
5. Elektroniczne pytanie o zgodę musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.
6. Zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie w sposób tak samo prosty i przystępny, w jaki została pozyskana.

§ 18.

Zgoda na przetwarzanie danych osobowych nie jest wymagana w przypadku, gdy dane będą przetwarzane:

a) w związku z zawarciem umowy z osobą, której dane dotyczą;
b) na podstawie przepisu prawa;
c) w interesie publicznym;
d) w prawnie usprawiedliwionym celu administratora danych;
e) w przypadku żywotnego interesu osoby, której dane dotyczą, gdy pozyskanie zgody jest konieczne, ale niemożliwe.

§ 19.

W celu zapewnienia należytej ochrony przetwarzania danych osobowych, u ADO zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych.

§ 20.

1. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w zabezpieczonych pomieszczeniach.
2. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce.
3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (Ms Word), arkuszach kalkulacyjnych (Ms Excel) lub programach równorzędnych (np. Open Office) i innych programach do tworzenia baz danych oraz w systemach informatycznych, np. system bankowości elektronicznej itp. stosuje się środki ochrony przed szkodliwym oprogramowaniem.
5. W przypadku wystąpienia konieczności dostępu do zbioru danych osobowych w czasie nieobecności pracownika upoważnionego do przetwarzania danych w tym zbiorze, ADO w zakresie dostępu do systemu informatycznego, może udostępnić ten zbiór innemu pracownikowi w celu dokonania niezbędnych czynności służbowych. Po powrocie nieobecny pracownik otrzymuje nowe indywidualne hasło dostępu.
6. W przypadku korzystania przez kilka osób z jednego komputera, w różnych ramach czasowych, każdy użytkownik ma własny profil z zakresem dostępu do danych odpowiadającym treści upoważnienia do przetwarzania danych.
7. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
8. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej niż 3 minuty nieaktywności pracy użytkownika (wygaszacz).

§ 21.

1. Opracowano i wdrożono Politykę Ochrony Danych Osobowych służącą do przetwarzania danych osobowych u ADO.
2. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony tych danych oraz odbyły szkolenie „Podstawy 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).”
3. Wszyscy Użytkownicy komputerów zostali przeszkoleni w zakresie zasad korzystania i zabezpieczeń jednostki.
4. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO oraz które podpisały oświadczenie o zachowaniu poufności zobowiązujące je do zachowania przetwarzanych danych w tajemnicy.
5. Prowadzone są wykazy osób i podmiotów, którym udostępniono lub powierzono przetwarzanie danych osobowych.

6. Przetwarzanie danych osobowych przez osoby upoważnione odbywa się w wyznaczonych pomieszczeniach, w godzinach pracy ADO.
7. Dostęp osób nieposiadających stosownych upoważnień do pomieszczeń, w których przetwarzane są dane osobowe odbywa się wyłącznie za zgodą ADO lub w obecności i pod nadzorem osób upoważnionych.

§ 22.

Zakres czynności dla osoby upoważnionej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę przetwarzanych danych osobowych w stopniu adekwatnym do jej zadań.

§ 23.

1. Nadzór nad dostępem do pomieszczeń, w których przetwarzane są dane osobowe sprawuje IODO lub wyznaczona przez niego osoba.
2. Pracownicy ADO są zobowiązani do informowania IODO o zauważonych próbach nieuprawnionego dostępu do pomieszczeń, w których przetwarzane są dane osobowe.

§ 24.

1. Osoby opuszczające puste pomieszczenie, w którym przetwarzane są dane osobowe, zobowiązane są do zamknięcia drzwi na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie, za wyjątkiem sytuacji związanych z ochroną przeciwpożarową.
2. Zabrania się samowolnego dorabiania kluczy do budynku/pomieszczeń ADO. Każdorazowa potrzeba dorobienia dodatkowego klucza lub kluczy winna być zgłoszona ADO, który wyraża na to zgodę oraz określa zasady wykonania raz posługiwania się kopią klucza/kluczy.
3. Po zakończeniu pracy pracownik zobowiązany jest :
    a) wylogować się z systemu/programu, w którym pracował;
    b) wyłączyć komputer poprzez prawidłową ścieżkę zamknięcia;
    c) zamknąć okna w pomieszczeniu,
    d) umieścić materiały i dokumenty zawierające dane osobowe w szafach lub szufladach zamykanych na klucz,
    e) zgodnie z zasadą czystego biurka, czystej drukarki i czystej kopiarki zniszczyć w niszczarce wszystkie materiały zbędne w postaci błędnie utworzonej lub niepotrzebnej dokumentacji mającej krótkotrwałe znaczenie praktyczne, m.in. wydruków komputerowych i innych materiałów analogowych zawierających dane osobowe.

§ 25.

1. Udostępnianie drogą pocztową lub kurierską dokumentów i materiałów zawierających dane osobowe może odbywać się przesyłką rejestrowaną, a w przypadku danych zawartych na nośnikach magnetycznych, optycznych lub elektronicznych – przesyłką rejestrowaną za potwierdzeniem odbioru.

2. Pracownicy ADO przygotowujący przesyłki, o których mowa w ust. 1 powinni dołożyć należytej staranności celem zabezpieczenia ich zawartości przed nieuprawnionym dostępem do ich zawartości osób trzecich.
3. U ADO dopuszcza się stosowanie zabezpieczeń technicznych i organizacyjnych innych, niż wymienione w Polityce Ochrony.

§ 26.

1. Sprawdzenia zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznych regulacji obowiązujących w tym zakresie u ADO dokonuje IODO.
2. IODO przeprowadza sprawdzenia w trybie sprawdzenia planowego, tj. według planu sprawdzeń, który określa przedmiot, zakres i termin przeprowadzenia poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania.
3. W przypadku otrzymania informacji o naruszeniu bezpieczeństwa danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, IODO przeprowadza niezwłocznie sprawdzenie doraźne.
4. Sprawdzeniu podlega każdy program, w którym przetwarzane są dane osobowe, zabezpieczenia fizyczne i organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami prawnymi.
5. IODO przygotowuje plan sprawdzeń na okres roku. Plan obejmuje co najmniej dwa sprawdzenia i jest zatwierdzany przez ADO.
6. Dokumentowanie przez IODO czynności w toku sprawdzenia polega na tworzeniu materiałów w postaci papierowej lub elektronicznej w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i opracowania sprawozdania.
7. W sprawozdaniu IODO stwierdza, czy naruszone zostały przepisy o ochronie danych osobowych, a jeżeli tak, to jakie są planowane lub podjęte działania przywracające stan zgodny z prawem. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.
8. IODO przekazuje sprawozdanie ze sprawdzenia planowego do ADO nie później niż w terminie 14 dni od zakończenia sprawdzenia. Sprawozdanie ze sprawdzenia doraźnego przekazywane jest niezwłocznie po zakończeniu sprawdzenia.

§ 27.

1. Za zapewnienie pracownikom warunków organizacyjnych mających na celu zapewnienie należytego bezpieczeństwa danych osobowych odpowiada ADO.
2. Na pracownikach oraz osobach upoważnionych do przetwarzania danych osobowych, w zakresie ich uprawnień i odpowiedzialności, ciąży obowiązek dbałości o zabezpieczanie danych osobowych przed ich udostępnieniem, zabraniem, przetwarzaniem z naruszeniem ustawy przez osoby nieuprawnione oraz zmianą, uszkodzeniem, utratą lub zniszczeniem.

§ 28.

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z przepisów prawa powszechnie obowiązującego.
2. Naruszenie zasad Polityki Ochrony Danych Osobowych stanowi incydent, o którym powinien być niezwłocznie powiadomiony IODO. O podjęciu działań naprawczych decyduje ADO na podstawie projektu działań opracowanego przez IODO.
3. Łamanie zasad wynikających z niniejszej Politycy Ochrony może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych i może skutkować nałożeniem kary porządkowej na zasadach określonych w przepisach prawa pracy, w szczególności w przypadku osoby, która po stwierdzeniu naruszenia bezpieczeństwa danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie IODO.
4. Udokumentowane umyślne złamanie zasad określonych w Polityce Ochrony jest traktowane jako ciężkie naruszenie obowiązków pracowniczych uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia z winy pracownika.

Rozdział 4.
Ogólne warunki korzystania z systemu informatycznego/ sprzętu komputerowego.

§ 29

Zasady zachowania bezpieczeństwa obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji przed ich nieuprawnionym przetwarzaniem.

§ 30

1. Zabrania się Użytkownikowi systemu Informatycznego/programu/komputera podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń tego systemu.
2. W celu zapobieżenia nieautoryzowanemu dostępowi Użytkownik nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom.
3. Zabronione jest korzystanie z systemu informatycznego/komputera z użyciem danych dostępowych innego Użytkownika.
4. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.
5. Użytkownik zobowiązany jest do przestrzegania zasady „czystego biurka”, w szczególności przed opuszczeniem swego stanowiska pracy powinien schować wszelkie dokumenty oraz informatyczne nośniki danych.
6. W czasie kopiowania, drukowania dokumentów zawierających dane osobowe, Użytkownik zobowiązany jest do zachowania zasady „czystej drukarki”, „czystej

kopiarki", w szczególności przed opuszczeniem stanowiska kopiowania/drukowania upewnić się, że w urządzeniach nie pozostały dokumenty zawierające dane osobowe.

7. Przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych z użyciem urządzeń mobilnych, Użytkownik jest zobowiązany do sprawdzenia, czy posiadane przez niego dane są należycie zabezpieczone przed dostępem osób nieupoważnionych.
8. Po zakończeniu przetwarzania danych osobowych, Użytkownik zobowiązany jest do należytego zabezpieczenia ich przed dostępem osób nieupoważnionych.

Rozdział 5.
Poczta elektroniczna.

§ 31.

Użytkownik zobowiązany jest do dbania o bezpieczeństwo poczty elektronicznej, w szczególności do używania hasła dostępu, nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł oraz zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.

Rozdział 6.
Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych.

§ 32.

1. Ryzyko w zakresie bezpieczeństwa danych osobowych, definiuje się jako prawdopodobieństwo wystąpienia zagrożeń i powstanie szkód, zniszczeń oraz przerw lub zakłóceń prawidłowego przetwarzania danych osobowych.
2. Zarządzanie ryzykiem jest procesem identyfikacji zasobów, odpowiadających im podatności i zagrożeń, oceny prawdopodobieństwa ich wystąpienia, wielkości potencjalnych strat oraz przeciwdziałania i określenia kryteriów akceptowalności ryzyka.
3. Zarządzanie ryzykiem obejmuje możliwie jak najszybszą identyfikację ryzyka związanego z planowanym działaniem, ocenę stopnia wpływu ryzyka na uzyskane wyniki lub cele oraz zastosowanie odpowiednich środków kontroli ryzyka.
4. Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, odnoszącym się do działalności ADO, dokonywany jest przez IODO.
5. Narzędziem wsparcia w tym procesie jest Plan zarządzania ryzykiem w zakresie bezpieczeństwa danych osobowych zawierający ryzyka zidentyfikowane dla ADO, przy czym katalog zidentyfikowanych ryzyk jest zbiorem otwartym, który może ulegać zmianom w zależności od warunków funkcjonowania ADO.
6. Pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na

realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko.

§ 33

1. IODO przeprowadza ocenę ryzyk po każdorazowym wystąpieniu incydentu oraz każdorazowej zmianie mogącej wpływać na poziom ryzyka, w tym szczególnie zmianie struktury organizacyjnej, otoczenia dotyczącego realizacji umów z nowymi podmiotami, technologii, infrastruktury, pracowników, metod pracy, przepisów prawa.
2. Niezwłocznie po wystąpieniu incydentu, IODO przedstawia ADO wyniki oceny zidentyfikowanych ryzyk wraz z propozycjami działań korygujących i zapobiegawczych, do których należy w szczególności: określenie zadań do realizacji, zdefiniowanie odpowiedzialności, ram czasowych oraz propozycji zmian celem poprawy bezpieczeństwa informacji.
3. Na podstawie raportów i sprawozdań otrzymanych ADO podejmuje ostateczną decyzję w zakresie realizacji działań zapewniających ochronę przetwarzanych informacji.
4. Do działań wskazanych w ust. 3 należy w szczególności:
    a) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
    b) utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
    c) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
    d) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
    e) dokonanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób upoważnionych;
    f) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
    g) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,
    h) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
    i) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
    j) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
    k) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

- dbałości o aktualizację systemu operacyjnego,
- minimalizowaniu ryzyka utraty informacji w wyniku awarii,
- ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
- zapewnieniu bezpieczeństwa plików systemowych,

- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- kontroli systemów teleinformatycznych,
- bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w sposób, umożliwiający szybkie podjęcie działań korygujących.

§ 34.

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    - próby naruszenia ochrony danych:
    - -z zewnątrz -włamania do systemu, podsłuch, kradzież danych,
    - -z wewnątrz -nieumyślna lub celowa modyfikacja danych, kradzież danych;
    - programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne;
    - awarie sprzętu lub uszkodzenie oprogramowania;
    - zabór sprzętu lub nośników z ważnymi danymi;
    - inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych;
    - usiłowanie zakłócenia działania systemu informatycznego.
2. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:

- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów, niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
- zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
- zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania,
- użytkowników, utrata/zagubienie danych),
- umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:

- zgłoszenia od Użytkowników,
- alarmy z systemów informatycznych,
- analizy incydentów,
- wyniki audytów / kontroli.

§ 35.

Każdy Pracownik/Osoba upoważniona, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Inspektora Ochrony Danych Osobowych. Zasady działania w przypadku zagrożenia lub naruszenia:

Kod zagrożenia lub naruszenia	Naruszenie lub zagrożenie nieświadome wewnętrzne i zewnętrzne	Postępowanie
1	Pomieszczenie, w którym przechowywane są dane osobowy pozostaje bez nadzoru	Należy zabezpieczyć dane osobowe – powiadomić ADO, IODO.
2	Komputer nie jest zabezpieczony hasłem	Należy zabezpieczyć dane osobowe – powiadomić ADO, IODO.
3	Dostęp do danych uzyskały osoby nieupoważnione – również w systemie informatycznym	Należy uniemożliwić dostęp osób bez upoważnienia – powiadomić ADO, IODO.
4	Próba kradzieży danych w formie papierowej	Należy nie dopuścić do kradzieży danych i powiadomić ADO, IODO.
5	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania	Należy powiadomić ADO, IODO.
6	Brak aktywnego oprogramowania antywirusowego	Należy powiadomić ADO, IODO, który zleci zaktualizowanie oprogramowania antywirusowego
7	Zniszczenie lub modyfikacja danych osobowych w formie papierowej	Należy zabezpieczyć dowody i powiadomić ADO, IODO którzy sprawdzą stan uszkodzeń.
8	Uszkodzenie komputerów, nośników danych	Należy powiadomić ADO, IODO, którzy w porozumieniu z obsługą informatyczną zabezpiecza dowodu i ocenia czy doszło do zniszczenia danych/ przywraca kopie zapasową
9	Zdarzenie losowe	IODO dokonuje oszacowania strat, powiadamia ADO.

10	Próba włamania/ włamanie do pomieszczenia/budynku – siedziby	Należy zabezpieczyć dowody powiadomić policję oraz ADO, IODO. IODO sprawdza stan uszkodzeń.

Z każdego incydentu IODO sporządza protokół i przedstawia go ADO.

§ 36.

1. W przypadku stwierdzenia wystąpienia zagrożenia, IODO prowadzi postępowanie wyjaśniające przy współpracy z ADO, w toku którego ustala zakres i przyczyny zagrożenia oraz jego potencjalne skutki, inicjuje ewentualne działania dyscyplinarne, rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości, dokumentuje prowadzone postępowania.
2. W przypadku stwierdzenia incydentu (naruszenia) IODO prowadzi postępowanie wyjaśniające, w toku którego:
    1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
    2) ustala osoby odpowiedzialne za naruszenie;
    3) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości; 4) dokumentuje prowadzone postępowania.
3. IODO jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Gdy stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa źródło powstania incydentu, zagrożenia lub słabości, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną.
4. IODO jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.
5. IODO prowadzi rejestr incydentów i zagrożeń według wzoru określonego w Załączniku nr 6 do niniejszej Polityki.

Rozdział 6.
Postanowienia końcowe

§ 39.

1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy regulujące tematykę ochrony danych osobowych.