INSTRUKCJA POSTĘPOWANIA
W PRZYPADKU NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

Przedszkole w Bolszewie

Metryka dokumentu

Data	Wersja	Opis zmiany	Autor
18.05.2018 r.	1.0	Stworzenie dokumentu	Podmiot zewnętrzny MBM Sp. z o.o. z siedzibą w Białymstoku Zarządzenie nr z dnia 18.05.2018 r.
02.09.2019 r.	2.0.	Aktualizacja dokumentu	Inspektor Ochrony Danych Białymstoku Zarządzenie nr 1 z dnia 02.09.2019 r.
31.08.2021 r.	3.0.	Aktualizacja dokumentu	Inspektor Ochrony D Zarządzenie nr z dnia 31.08.2021 r.

Dokument przygotował

Imię i nazwisko	Stanowisko	Podpis
Imię i nazwisko	Stanowisko	Podpis
Monika Wegner	Inspektor Ochrony Danych	
Sławomir Łągiewczyk	Administrator Systemów Informatycznych	

Dokument zatwierdził

Data	Podpis
Administrator Danych Osobowych	

ROZDZIAŁ 1
Postanowienia ogólne

§ 1

Celem **Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych** zwaną dalej „Instrukcją", jest aktywna kontrola nad przypadkami naruszeń i podejrzeniami naruszeń w celu zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych osobowych. Przestrzeganie postanowień niniejszej Instrukcji służyć ma wykrywaniu i właściwemu reagowaniu na przypadki naruszenia ochrony danych osobowych.

§ 2

1. Osobą sprawującą nadzór nad przestrzeganiem zasad ochrony danych osobowych oraz odpowiedzialną za nadzorowanie przypadków naruszeń jest Inspektor Ochrony Danych.
2. Osobą sprawującą nadzór nad przetwarzaniem danych w systemach informatycznych oraz sprawującą kontrolę i ocenę funkcjonowania mechanizmów technicznych zabezpieczeń systemów informatycznych służących do przetwarzania danych jest Administrator Systemów Informatycznych we współpracy z Inspektorem Ochrony Danych**.**

ROZDZIAŁ 2
Definicje

§ 3

Przez użyte w Instrukcji określenia należy rozumieć:

1. **Administrator danych osobowych (ADO –** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
2. **Rozporządzenie** – rozporządzenie Parlamentu Europejskiego i Rady 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 osobowych) (Dz. Urz. UE L 119 z 04.05.2016 , str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) zwana dalej także RODO;

3. **Ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych zwana w dalszej części ustawą;
4. **Inspektor ochrony danych –** rozumie się przez to osobę wyznaczoną przez administratora danych osobowych, posiadającą odpowiednie kwalifikacje zawodowe, wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych powołaną w celu informowania i doradzania Administratorowi, podmiotowi przetwarzającemu oraz pracownikom w zakresie obowiązującego prawa o ochronie danych oraz niniejszej polityki jak również w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla podmiotów przetwarzających i organu nadzorczego.
5. **Administrator systemu informatycznego -** pracownik lub podmiot zewnętrzny odpowiedzialny za prawidłową pracę systemów informatycznych, w tym utrzymanie ciągłości działania oraz bezpieczeństwa w infrastrukturze informatycznej, inwentaryzowanie, okresowe sprawdzanie stanu urządzeń oraz sprzętu pozwalającego na obsługę czynności przetwarzania danych osobowych w systemach informatycznych.
6. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7. **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
8. **Przetwarzanie danych –** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
9. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
10. **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
11. **Osoba upoważniona do przetwarzania danych osobowych lub użytkownik** – każda osoba świadcząca na rzecz Administratora pracę lub usługi w oparciu o jakikolwiek

stosunek prawny, jeżeli to świadczenie pracy lub usług wiąże się z przetwarzaniem danych osobowych, posiadająca imienne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator jeżeli dane są przetwarzane w systemie informatycznym.

12. **Zabezpieczenie danych** – zabezpieczenie danych poprzez wdrożenie i eksploatację środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
13. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
14. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów oraz narzędzi programowych zastosowanych w celu przetwarzania danych.
15. **Elektroniczny nośnik danych** – materiał lub urządzenie służące do zapisywania, przechowywania lub odczytywania danych osobowych w postaci cyfrowej lub analogowej;
16. **System tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przewarzaniem informacji oraz wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.
17. **Sieć lokalna** – połączenie systemów informatycznych administratora wyłącznie dla jego własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
18. **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący użytkownika upoważnionego do przetwarzania danych w systemie informatycznym.
19. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Administratorowi oraz Użytkownikowi upoważnionemu do Przetwarzania Danych w Systemie informatycznym.
20. **Uwierzytelnianie** – proces, którego celem jest weryfikacja tożsamości deklarowanej przez Użytkownika.
21. **Pomieszczenia** – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego lub mobilnego sprzętu komputerowego oraz w systemie tradycyjnym.
22. **Uchybienie** - świadome lub nieświadome działania zmierzające do zagrożenia wskutek, których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych;
23. **Zagrożenie** - świadome lub nieświadome działania wskutek, których doszło do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.
24. **poufność danych –** właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom;
25. **integralność danych –** właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

26. **rozliczalność danych –** właściwość zapewniająca, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
27. **integralność systemu –** rozumiana jest jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
28. **dostępność informacji –** zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
29. **uchybienie** - świadome lub nieświadome działania zmierzające do zagrożenia wskutek, których może dojść do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych;
30. **Przedszkole w Bolszewie - Przedszkole w Bolszewie** z siedzibą – 84-239 Bolszewo, ul. Leśna 35
31. **Dyrektor –** Dyrektor Przedszkola w Bolszewie

ROZDZIAŁ 3
Identyfikacja naruszeń

§ 4

Do głównych zagrożeń mających wpływ na bezpieczeństwo ochrony danych osobowych należy zaliczyć:

1) **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu, awarie serwerów) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu informatycznego, zostaje zakłócona ciągłość systemu, ale nie dochodzi do utraty poufności danych.
2) **Zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki informatyczne, pomyłki ludzkie, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu lub oprogramowania, niewłaściwe zabezpieczenie pomieszczeń lub sprzętu) – ich występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu i może dojść do naruszenia poufności danych.
3) **Zagrożenia zamierzone** – (świadome i celowe działania np. włamanie do systemu - nieuprawniony dostęp do systemu z zewnątrz, działanie wirusów komputerowych - nieuprawniony dostęp do systemu z wewnątrz, udostępnienie danych osobie nieupoważnionej, kradzież sprzętu informatycznego zawierającego dane, świadome zniszczenie danych) – ich występowanie powoduje naruszenie poufności danych, ale z reguły nie powoduje uszkodzenia infrastruktury technicznej i zakłócenia ciągłości pracy.

§ 5

Naruszenie ochrony danych osobowych może być spowodowane:

1) oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;

2) niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;
3) umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania użytkowników przetwarzających dane osobowe.

§ 6

Za naruszenie lub podejrzenie naruszenia bezpieczeństwa danych osobowych uważa się przede wszystkim:

1) losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.);
2) niewłaściwe parametry środowiska (nadmierna wilgotność, wysoka temperatura, oddziaływanie pola elektromagnetycznego, wibracje lub wstrząsy wywołane urządzeniami przemysłowymi);
3) awarię sprzętu lub oprogramowania, która wyraźnie wskazuje na umyślne działanie w kierunku naruszenia danych, a także niewłaściwe działalnie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
6) stwierdzenie próby modyfikacji lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia;
7) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń. Ujawnienie osobom nieuprawnionym danych osobowych obejmuje również przesłanie dokumentu lub wiadomości zawierającej dane osobowe do nieuprawnionego adresata;
8) ujawnienie istnienia nieautoryzowanych kont dostępu do systemu informatycznego służącego do przetwarzania danych osobowych;
9) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub niedozwolone skasowanie lub skopiowanie danych osobowych, w tym stosowanie nieodpowiednich technik usuwania danych.
10) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa (np. niewylogowanie się z systemu przed opuszczeniem stanowiska pracy; pozostawienie otwartego pomieszczenia bez nadzoru osób upoważnionych do przetwarzania danych osobowych; brak zmiany hasła do systemów informatycznych przez okres dłuższy niż 3 miesiące; pozostawianie kluczy do pomieszczeń po zakończeniu pracy w sposób umożliwiający dostęp do kluczy przez osoby nieupoważnione do przetwarzania danych osobowych; pozostawianie na wymienniku dokumentów zawierających dane osobowe, co do których dostęp możliwy będzie także dla innych pracowników (nieupoważnionych do przetwarzania danych));
11) brak dostępu do zawartości zbioru danych – zbiór istnieje, lecz nie można go otworzyć;
12) informacja o zainfekowaniu systemu wirusami;
13) brak urządzeń systemu lub nośników informacji, na których zapisane są dane osobowe;
14) utrata możliwości fizycznego dostępu do danych (np. zagubiony klucz do pomieszczenia lub mebli biurowych);

15) próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia, w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu;
16) zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych.
17) nieuprawnione prace na koncie użytkownika dopuszczonego do przetwarzania danych osobowych przez osobę do tego nieuprawnioną;
18) ujawnienie indywidualnych haseł dostępu użytkowników do systemu;
19) niewykonanie kopii bezpieczeństwa w odpowiednim terminie;
20) pozostawienie bez opieki dokumentacji w miejscu dostępnym dla osób nieupoważnionych do przewarzania danych osobowych.

ROZDZIAŁ 4
Procedury postępowania w przypadku naruszeń

§ 7

1. Każdy użytkownik w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie systemu ochrony, o których mowa w § 6 niniejszej Instrukcji, zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Inspektora Ochrony Danych oraz w razie potrzeby Administratora Systemów Informatycznych.

2. W razie braku możliwości zawiadomienia Inspektora Ochrony Danych, należy zawiadomić bezpośredniego przełożonego, którego obowiązkiem jest zawiadomienie Administratora Danych Osobowych oraz w razie potrzeby Administratora Systemów Informatycnych.

3. Do czasu przybycia na miejsce osoby nadzorującej przypadki naruszeń użytkownik powinien:
   1) niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony (o ile to jest możliwe), a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać – o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić analizę i dokumentację danego przypadku,
   4) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych,
   5) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu;
   6) podjąć stosowne działania, jeżeli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej.
   7) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku.
   8) ustalić przyczynę i sprawcę naruszenia ochrony oraz zapisać wszelkie informacje i okoliczności związane ze zdarzeniem,
   9) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia,
   10) zabezpieczyć dostęp do pomieszczenia lub urządzenia.

4. Dokonywanie zmian w miejscu naruszenia ochrony danych osobowych jest dopuszczalne tylko w wypadku konieczności ratowania osób, mienia albo zapobiegania powstaniu innego niebezpieczeństwa zmierzającego do dalszego naruszenia bezpieczeństwa ochrony danych.

5. W przypadku stwierdzenia przez użytkownika naruszenia bezpieczeństwa danych w systemie informatycznym należy dodatkowo:
   1) zabezpieczyć system informatyczny;
   2) zabezpieczyć technicznie stan urządzeń;
   3) zabezpieczyć zawartość zbioru danych osobowych;
   4) fizycznie odłączyć urządzenia i te segmenty sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
   5) wylogować użytkownika podejrzanego o naruszenie bezpieczeństwa zabezpieczenia ochrony danych.
   6) w razie potrzeby zmienić hasło dla administratora

§ 8

W przypadku uszkodzenia urządzeń służących do przetwarzania danych, utraty danych lub ich zniekształcenia, odtwarza się bazy danych osobowych z kopii bezpieczeństwa.

§ 9

1. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych osoba odpowiedzialna za nadzór nad naruszeniami podejmuje następujące kroki:
   1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy,
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej lub odpowiedzialnej za naruszenie jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem
   3) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia bezpieczeństwa danych (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci, programów, zbiorów danych itp.),
   4) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   5) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
   6) rozważa celowość i potrzebę zawiadomienia o zaistniałym naruszeniu Administratora Danych Osobowych.
   7) nawiązuje bezpośredni kontakt ze specjalistami spoza Urzędu (jeśli zachodzi taka potrzeba),
   8) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,
   9) po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych);
   10) dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport, którego wzór stanowi **zał. nr 1** do niniejszej Instrukcji.

11) w przypadku naruszenia ochrony danych osobowych, które skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych zawiadamia o naruszeniu Urząd Ochrony Danych Osobowych.
12) w przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych przygotowuje zawiadomienie o takim naruszeniu, które Administrator Danych Osobowych przekazuje osobie, której dane dotyczą.

2. W przypadku naruszenia danych w systemie informatycznym Inspektor Ochrony Danych wraz z Administratorem Systemów Informatycznych dodatkowo:

1) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
2) w celu powstrzymania lub ograniczenia dostępu do danych osoby nieupoważnionej podejmuje odpowiednie kroki zmierzające do: fizycznego odłączenia urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do zbiorów danych osobie nieupoważnionej, wylogowania użytkownika systemu podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmiany hasła poprzez które uzyskano nielegalny dostęp, aby uniknąć ponownej próby włamania,
3) przywraca prawidłowy stan działania systemu,
4) sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
5) wyraża zgodę na ponowne uruchomienie komputera lub innych urządzeń.

§ 9

1. Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych podejmują niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

1) Jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub inny atak sieciowy, jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie zlecają przeprowadzenie przeglądów oraz konserwacji urządzeń i programów, ustalenie źródła pochodzenia wirusa komputerowego lub innego ataku sieciowego oraz wdrożenie skuteczniejszego zabezpieczenia antywirusowego, a w miarę potrzeby kontaktują się z dostawcą usług telekomunikacyjnych w celu usprawnienia systemu zabezpieczeń.
2) Jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, Inspektor Ochrony Danych przeprowadza dodatkowe kursy i szkolenia osób upoważnionych do przetwarzania danych osobowych, a wobec osób winnych zaniedbań wnioskuje o wyciągnięcie konsekwencji przewidzianych prawem.
3) jeżeli przyczyną zdarzenia było włamanie, w celu nielegalnego pozyskania danych dokonuje szczegółowej analizy wdrożonych środków zabezpieczenia i proponuje wdrożenie skuteczniejszej ochrony fizycznej.
4) Jeżeli przyczyną zdarzenia był czyn zabroniony lub zachodzi jego uzasadnione podejrzenie, zawiadamia organy ścigania.

§ 10

1. Inspektor Ochrony Danych prowadzi rejestr naruszeń, który stanowi **zał. nr 2** do niniejszej Instrukcji przy czym dopuszcza się możliwość prowadzenia rejestru w formie elektronicznej
2. Inspektor Ochrony Danych wraz z Administratorem Systemów Informatycznych dokonuje rocznej analizy przypadków naruszeń. Dokument do analizy naruszeń stanowi **zał. nr 3** do niniejszej Instrukcji.

ROZDZIAŁ 5
Postanowienia końcowe

§ 11

1. Każdy użytkownik przetwarzający dane osobowe w zbiorach danych zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować przepisy w niej zawarte na swoim stanowisku pracy.
2. Nieprzestrzeganie zasad wskazanych w niniejszej Instrukcji stanowi niewykonanie bądź nienależyte wykonanie obowiązków pracowniczych lub niewykonanie bądź nienależyte wykonanie innej niż umowa o pracę umowy stanowiącej podstawę zatrudnienia, co może wiązać się dla osoby zatrudnionej z odpowiedzialnością majątkową wobec administratora danych.
3. Nadużycie przez użytkownika postanowień niniejszej Instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

§ 12

W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy Rozporządzenia Parlamentu Europejskiego i Rady 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 osobowych) oraz przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Administrator Danych Osobowych

załącznik nr 1

RAPORT Z NARUSZENIA
BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Nr raportu ……/……. Data i godzina wystąpienia zdarzenia

.....

Miejsce wystąpienia zdarzenia

.....

Osoba zawiadamiająca

……..…….

……..

Opis zdarzenia i rodzaj naruszenia

.....

.....

.....

.....

.....

Przyczyny powstania zdarzenia

.....

.....

.....

.....

Zaistniałe skutki zagrożenia

.....

.....

.....

.....

.....

.....

.....

.....

Podjęte czynności naprawczo-zapobiegawcze

.....

.....

.....

.....

.....

Osoby zaangażowane w wyjaśnienie zdarzenia

……..……

……..

Podpisy:

……..…….

Osoba zgłaszająca

……

Osoba nadzorująca

załącznik nr 2

REJESTR NARUSZEŃ

L.P	Data i numer raportu	Data i godzina wystąpienia zdarzenia	Rodzaj naruszenia	Informacja o zawiadomieniu UODO

załącznik nr 3

ROCZNA ANALIZA PRZYPADKÓW NARUSZEŃ

Data sporządzenia analizy .....

Osoba nadzorująca

……..……

Ilość naruszeń ……. w tym: uchybienia …… zagrożenia ……..

1) Ocena wdrożonych zabezpieczeń zapobiegających naruszeniom

.....

.....

.....

.....

2) Ocena realizacji działań naprawczo-zapobiegawczych

.....

.....

.....

.....

3) Zadania do realizacji w celu zapobiegania naruszeniom

.....

.....

.....

.....

.....

Podpisy:

……..……

Osoba nadzorująca

……..

Osoba przyjmująca raport