INSTRUKCJA

POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH OSOBOWYCH
**W PRZEDSZKOLU NR 62 STUMILOWY LAS WE WROCŁAWIU.**

Niniejszy dokument jest własnością Przedszkola Nr 62

Zabrania się kopiowania, rozpowszechniania oraz dokonywania zmian treści bez zgody Dyrektora Przedszkola

do użytku służbowego

SPIS TREŚCI

[ROZDZIAŁ I POSTANOWIENIA OGÓLNE 3](#_Toc522732164)

[ROZDZIAŁ II POSTĘPOWANIE WYJAŚNIAJĄCE 7](#_Toc522732165)

[ROZDZIAŁ III ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH DO ORGANU NADZORCZEGO 10](#_Toc522732166)

[ROZDZIAŁ IV POSTANOWIENIA KOŃCOWE 14](#_Toc522732167)

ROZDZIAŁ I POSTANOWIENIA OGÓLNE

* 1. **Wstęp**
		1. Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych
		w Przedszkolu Nr 62 „Stumilowy Las” we Wrocławiu (dalej Przedszkole Nr 62) zwana dalej „Instrukcją”, określa zasady postępowania w przypadku, gdy:
1. stwierdzono naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych lub na innych nośnikach informacji, w tym nośnikach papierowych;
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zasad ochrony danych osobowych.
	* 1. Naruszenie ochrony danych osobowych może być skutkiem:
3. szkodliwego wpływu środowiska na przetwarzanie danych osobowych, zarówno
w systemie informatycznym, jak i w pomieszczeniach, w których przetwarza się dane osobowe w formie papierowej;
4. zewnętrznych zdarzeń losowych;
5. zamierzonych lub niezamierzonych nieuprawnionych działań osób upoważnionych do przetwarzania danych osobowych;
6. nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych.
	* 1. Do stosowania Instrukcji zobowiązani są wszyscy pracownicy Przedszkola Nr 62.
	1. **Rodzaje naruszenia zasad ochrony danych osobowych i symptomy świadczące
	o możliwości naruszenia**
		1. Rodzaje naruszeń ochrony danych osobowych

Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:

1. nieupoważniony dostęp, modyfikację, kopiowanie, zniszczenie lub usunięcie danych osobowych zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych;
2. udostępnianie danych osobowych podmiotom i osobom nieuprawnionym;
3. nielegalne (świadome lub nieświadome) ujawnienie danych osobowych;
4. przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem;
5. nieautoryzowany dostęp do pomieszczeń, w których przetwarza się dane osobowe;
6. niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych, w tym w szczególności:
	* 1. pozostawienie kopii danych osobowych bez nadzoru;
		2. niezablokowanie dostępu do systemu informatycznego służącego do przetwarzania danych osobowych (stacja robocza, serwer);
		3. brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi do samodzielnego przebywania w obszarze przetwarzania danych osobowych;
7. nieautoryzowany dostęp do danych osobowych przez połączenie sieciowe;
8. wykrycie niezabezpieczonego kanału dystrybucji danych osobowych;
9. stwierdzenie obecności wirusów komputerowych lub innych programów naruszających integralność systemu informatycznego służącego do przetwarzania danych osobowych;
10. ujawnienie indywidualnych haseł dostępu do systemu informatycznego służącego do przetwarzania danych osobowych;
11. przesyłanie danych osobowych przez Internet bez zabezpieczenia;
12. wykonanie nieuprawnionych kopii danych osobowych;
13. naruszenie bezpieczeństwa kopii danych osobowych;
14. kradzież nośników zawierających dane osobowe;
15. kradzież komponentów fizycznych systemu informatycznego służącego do przetwarzania danych osobowych;
16. utrata danych osobowych przetwarzanych w systemie informatycznym lub przechowywanych na zewnętrznych nośnikach elektronicznych;
17. brak aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii;
18. niewłaściwe zniszczenie nośników z danymi osobowymi, pozwalające na odczyt zapisanych na nich danych;
19. naruszenie zasad ochrony fizycznej obszaru przetwarzania danych osobowych;
20. dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień;
21. przydzielenie użytkownikowi uprawnień niezgodnych z wydanym upoważnieniem do dostępu do danych osobowych.
	* 1. Symptomy naruszenia ochrony danych osobowych

O możliwości zaistnienia przypadku naruszenia zasad ochrony danych osobowych mogą świadczyć m.in.:

1. nadmierne, w stosunku do wykonywanych zadań lub zakresu upoważnienia, uprawnienia użytkownika do zasobów systemu informatycznego służącego do przetwarzania danych osobowych;
2. niestabilna praca systemu, w którym przetwarza się dane osobowe;
3. korzystanie bez zgody przełożonego z zasobów systemu poza godzinami pracy;
4. nowe, budzące uzasadnione podejrzenia konta użytkowników systemu;
5. wysoka aktywność użytkowników kont, które dotychczas pozostawały niewykorzystane;
6. odnotowanie w krótkim czasie dużej liczby nieudanych prób logowania (przy zastrzeżeniu konfiguracji systemu nakazującej interwencję administratora systemu po trzech próbach podania błędnego hasła);
7. anomalie w pracy systemu lub jego logicznych komponentów (świadczące np.
o obecności wirusa lub złośliwego kodu);
8. naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych obszaru przetwarzania danych osobowych (wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się okna itp.)

ROZDZIAŁ II POSTĘPOWANIE WYJAŚNIAJĄCE

* 1. **Zgłaszanie naruszeń ochrony danych osobowych**
		1. Każdy kto podejrzewa lub stwierdzi naruszenie ochrony danych osobowych, ma obowiązek niezwłocznie:
1. powiadomić o zaistniałym zdarzeniu swojego bezpośredniego przełożonego oraz Inspektora ochrony danych;
2. powiadomić Informatyka w przypadku, gdy naruszenie miało związek
z przetwarzaniem danych w systemie informatycznym,
	* 1. Powiadomienie o podejrzeniu naruszenia ochrony danych osobowych należy przesłać za pośrednictwem służbowej poczty elektronicznej na adres mailowy lub przekazać telefonicznie lub osobiście Inspektorowi ochrony danych, jeżeli naruszenie miało związek z przetwarzaniem danych w systemach informatycznych.
		2. Powiadomienie, o którym mowa w pkt 2.1.2, powinno zawierać precyzyjne
		i wyczerpujące informacje, określające:
3. czas, miejsce i okoliczności zdarzenia;
4. symptomy świadczące o możliwości naruszenia ochrony danych osobowych;
5. inne okoliczności i fakty mogące pomóc w ustaleniu przyczyn naruszenia zasad ochrony danych osobowych.
	* 1. Wzór powiadomienia o naruszeniu ochrony danych osobowych określony jest
		w załączniku nr 1 do niniejszej Instrukcji.
		2. Każdy kto podejrzewa lub stwierdził naruszenie zasad ochrony danych osobowych ma obowiązek:

1) udzielać odpowiedzi na pytania związane z zaistniałą sytuacją inspektorowi ochrony danych,

1. powstrzymać się od dalszej pracy, w szczególności, gdy naruszenie miało miejsce
w systemie informatycznym, do momentu uzyskania stosownych wytycznych co do dalszej pracy, udzielonych przez Inspektora ochrony danych.
	1. **Postępowanie wyjaśniające**
		1. Postępowania wyjaśniające w sprawach dotyczących naruszenia ochrony danych osobowych w Przedszkolu Nr 62 prowadzi Inspektor ochrony danych.
		2. Po otrzymaniu powiadomienia, o którym mowa w pkt 2.1.2, Inspektor ochrony danych ocenia sytuację i podejmuje poniższe działania:
2. dokonuje rozpoznania zdarzenia;
3. lokalizuje źródło problemu;
4. ocenia wagę problemu;
5. określa środki mające na celu likwidację skutków naruszenia oraz zapobiegawcze, chroniące przed wystąpieniem podobnego zdarzenia w przyszłości.
	* 1. W sytuacji naruszenia ochrony przetwarzania danych osobowych w systemie informatycznym, Inspektor ochrony danych wyjaśnia zdarzenie we współpracy
		z Informatykiem, ocenia sytuację i podejmuje odpowiednie do potrzeb działania, określone w pkt 2.1.6.
		2. Każdy zidentyfikowany incydent, naruszający ochronę danych osobowych, musi być rozpoznany i wyjaśniony w ciągu 24 godzin od momentu otrzymania zgłoszenia o jego wystąpieniu.
		3. Każde postępowanie wyjaśniające kończy się analizą skutków naruszenia
		i sporządzeniem raportu, zawierającego podjęte działania naprawcze oraz wnioski dotyczące w szczególności proponowanych działań zapobiegawczych, a także informację o konieczności podjęcia działań, o których mowa w pkt 3.2. lub 3.3 oraz 3.4.
		4. Raport, podpisany przez Inspektora ochrony danych oraz przekazywany jest niezwłocznie Dyrektorowi Przedszkola.
		5. Wzór raportu z postępowania wyjaśniającego określony jest w załączniku nr 2.
		6. W przypadku, gdy naruszenie danych osobowych, skutkowałoby ryzykiem naruszenia praw lub wolności osób fizycznych, Inspektor ochrony danych podejmuje działania określone w rozdziale III.
		7. Inspektor ochrony danych, stosownie do postanowień zawartych w art. 33 ust. 5, dokumentuje wszelkie naruszenia ochrony danych osobowych, w formie rejestru zgłoszonych incydentów.
		8. Rejestr, o którym mowa w pkt 2.2.9, zawiera w szczególności:
6. datę i godzinę zgłoszenia faktu naruszenia zabezpieczenia lub ujawnienia symptomów świadczących o podejrzeniu dokonania naruszenia ochrony danych osobowych;
7. nazwisko osoby zgłaszającej zdarzenie;
8. nazwisko osoby odpowiedzialnej za zaistnienie zdarzenia (o ile zostanie ustalone);
9. okoliczności naruszenia ochrony danych osobowych, w tym szczegółowy opis lub symptomy naruszenia;
10. skutki naruszenia;
11. opis podjętych działań zaradczych;
12. opis pozostałych działań i decyzji, jakie miały związek z wyjaśnieniem naruszenia, w tym informację o przesłaniu zgłoszenia naruszeniu do Administratora lub organu nadzorczego, a także o przesłaniu lub nie przesłaniu zawiadomienia do osób, których dane zostały naruszone.

ROZDZIAŁ III ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH DO ORGANU NADZORCZEGO

* 1. **Kwalifikacja incydentów**
		1. W przypadku, gdy zdarzenie dotyczące naruszenia ochrony danych osobowych przetwarzanych, niezależnie od tego czy miało miejsce w systemie informatycznym, czy dotyczyło przetwarzania danych w formie papierowej, zostanie zakwalifikowane przez Inspektora ochrony danych jako naruszenie podlegające zgłoszeniu do organu nadzorczego, Inspektor ochrony danych podejmuje działania określone
		w niniejszym rozdziale.
		2. Inspektor ochrony danych po otrzymaniu zgłoszenia dotyczącego naruszenia ochrony danych osobowych i przeprowadzeniu postępowania wyjaśniającego, o którym mowa w rozdziale II, kwalifikuje zaistniałe zdarzenie jako incydent podlegający zgłoszeniu do organu nadzorczego, zgodnie z art. 32 RODO, lub nie podlegający takiemu zgłoszeniu.
		3. Przy dokonywaniu kwalifikacji Inspektor ochrony danych bierze pod uwagę czy dane osobowe zostały udostępnione osobom nieuprawnionym, zabrane przez osobę nieuprawnioną, zniszczone lub zmodyfikowane w sposób mogący mieć wpływ na prawa lub wolność osoby, której dane uległy takiej modyfikacji lub zniszczeniu, w szczególności czy na zaistniałe zdarzenie pociąga za sobą ryzyko naruszenia praw lub wolności osoby, której dane dotyczyły.
		4. Po zakwalifikowaniu zdarzenia jako incydent podlegający zgłoszeniu do organu nadzorczego, Inspektor ochrony danych informuje Dyrektora Przedszkola, o zaistnieniu takiego zdarzenia i konieczności podjęcia stosownych działań, o których mowa w pkt 3.2 lub 3.3 oraz 3.4.
		5. Zgłoszenie, o naruszeniu, o którym mowa w pkt 3.1.4, musi zawierać w szczególności poniższe informacje:
1. 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;
2. zawierać imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4. opisywać środki zastosowane lub proponowane przez Administratora/Podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym
w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
	1. **Przesyłanie zgłoszeń do Administratora**
		1. W przypadku, gdy naruszenie, o którym mowa w pkt 3.1.4, dotyczyło danych,
		w stosunku do których Przedszkole Nr 62 jest Podmiotem przetwarzającym, Inspektor ochrony danych przygotowuje zgłoszenie, zgodnie ze wzorem określonym
		w załączniku nr 3.
		2. Zgłoszenie, o którym mowa wyżej, przedkłada do zatwierdzenia Dyrektorowi Przedszkola a następnie niezwłocznie, nie później jednak niż w ciągu 12 godzin
		z zastrzeżeniem pkt 3.2.3, przesyła podmiotowi, który jest Administratorem
		w stosunku do danych, których dotyczyło naruszenie, w trybie określonym w umowie powierzenia podpisanej z tym Administratorem.
		3. Jeżeli terminy przesyłania Administratorom zgłoszenia o naruszeniu, podlegającemu zgłoszeniu do organu nadzorczego, są określone w stosownych umowach powierzenia, podpisanych przez Przedszkole Nr 62 z poszczególnymi Administratorami oraz są inne niż termin, określony w niniejszej Instrukcji (tj. 36 godzin od stwierdzenia naruszenia), muszą być realizowane w terminach określonych w tych umowach.
		4. W przypadku, gdy naruszenie będzie pociągało za sobą obowiązek zawiadomienia osób, których dane zostały naruszone, zgłoszenie, o którym mowa w pkt 3.2.1, musi zawierać informację o takim obowiązku.
		5. W przypadku, o którym mowa w pkt 3.2.4, do zgłoszenia dołączany jest wówczas zawiadomienie,
		o którym mowa w pkt. 3.4.2.
	2. **Przesyłanie zgłoszeń do organu nadzorczego**
		1. W przypadku, gdy naruszenie, o którym mowa w pkt 3.1.4, dotyczyło danych,
		w stosunku do których Przedszkole Nr 62 jest Administratorem, Inspektor ochrony danych przygotowuje zgłoszenie, zgodnie ze wzorem określonym w załączniku nr 4.
		2. Zgłoszenie, o którym mowa wyżej, przedkłada do zatwierdzenia Dyrektorowi Przedszkola, a następnie wysyła to zgłoszenie, listem poleconym za potwierdzeniem zwrotnym odbioru, do organu nadzorczego.
		3. Zgłoszenie do organu nadzorczego musi być wysłane nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.
		4. W przypadku, gdy przesłanie zgłoszenia do organu nadzorczego nie może nastąpić
		w terminie, o którym mowa w pkt 3.3.3, do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia.
	3. **Przesyłanie zawiadomienia o naruszeniu do osób, których dane zostały naruszone**
		1. Jeżeli w wyniku prowadzonego przez Inspektora ochrony danych postępowania wyjaśniającego, dotyczącego incydentów, o których mowa w pkt 3.1.4, stwierdzone zostanie, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Inspektor ochrony danych przygotowuje zawiadomienie o takim naruszeniu do wszystkich osób, których dane dotyczą.
		2. Zawiadomienie, o którym mowa wyżej, powinno zawierać:
5. opis charakteru naruszenia ochrony danych osobowych, w tym czas, miejsce i opis wystąpienia zdarzenia, a także rodzaj danych jakie uległy naruszeniu;
6. imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych;
7. opis możliwych konsekwencji naruszenia ochrony danych osobowych;
8. opis zastosowanych lub proponowanych przez Administratora środków w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis podjętych środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
	* 1. Wzór zawiadomienia określony jest w załączniku nr 5.
		2. Zawiadomienia po zatwierdzeniu i podpisaniu przez Dyrektora Przedszkola powinny być bez zbędnej zwłoki przesłane do wszystkich osób, których dane zostały naruszone.
		3. Przesłanie zawiadomienia, o którym mowa w pkt 3.4.4, następuje wyłącznie
		w przypadku, gdy naruszeniu uległy dane, w stosunku do których Przedszkole Nr 62 jest Administratorem.
		4. W przypadku, gdy naruszenie dotyczy danych, w stosunku do których Przedszkole Nr 62 jest podmiotem przetwarzającym zawiadomienie, o którym mowa w pkt. 3.4.2, przesyłane jest do podmiotu będącego Administratorem tych danych wraz ze zgłoszeniem, o którym mowa w pkt 3.2.
		5. Zawiadomienie, o którym mowa w pkt 3.4.1, nie jest wymagane, w przypadkach, gdy
		w Przedszkolu Nr 62:
9. zostały przez wdrożone i zastosowane odpowiednie środki organizacyjne
i techniczne do ochrony danych osobowych, których dotyczy naruszenie,
w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
10. zastosowane zostały środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
11. wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku Przedszkole Nr 62 musi wydać publiczny komunikat (np. poprzez publikację na własnej stronie internetowej) lub zastosować inny środek (np. informacja telefoniczna), za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

ROZDZIAŁ IV POSTANOWIENIA KOŃCOWE

* 1. **Zachowanie poziomu bezpieczeństwa danych**
		1. Jeżeli w czasie usuwania skutków naruszenia ochrony danych osobowych nastąpi czasowe obniżenie poziomu ich bezpieczeństwa w szczególności, gdy będzie to miało miejsce w systemie informatycznym, to po zakończeniu czynności naprawczych system przetwarzający te dane powinien posiadać poziom bezpieczeństwa nie niższy niż poprzednio obowiązujący.
	2. **Odpowiedzialność za osób upoważnionych do przetwarzania danych**
		1. Każda osoba upoważniona do przetwarzania danych osobowych obowiązana jest zapoznać się z niniejszą Instrukcją oraz złożyć stosowne oświadczenie dotyczące znajomości zawartych w niej zasad.
		2. Za naruszenie obowiązków wynikających z Instrukcji grozi odpowiedzialność dyscyplinarna, określona w przepisach odrębnych.