POLITYKA

OCHRONY DANYCH OSOBOWYCH

w Szkole Podstawowej im. Marii Konopnickiej w Garbowie

Spis treści

1. Postanowienia ogólne:

Polityka Ochrony Danych Osobowych stanowi dokument wewnętrzny Szkoły Podstawowej w Garbowie, który jest objęty zachowaniem w poufności przez wszystkie osoby, którym zostanie przedstawiony. Każda osoba mająca dostęp do informacji zobowiązana jest zapoznać się z niniejszym dokumentem, podpisać oświadczenie potwierdzające znajomość jego treści, a także zobowiązanie do zachowania w tajemnicy danych, do których ma lub będzie miała dostęp. Wzór oświadczenia stanowi załącznik nr 1 do niniejszego dokumentu.

1.2. Podstawa prawna:

Polityka Ochrony Danych Osobowych wraz z załącznikami opiera się na:

1) Rozporządzeniu 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 (Dz.U. UE L.2016.119.1), zwanym w dalszej części RODO.
2) Ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2018 poz. 1000) zwaną w dalszej części UODO.
3) Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565).
4) Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526).

1.3. Podstawowe definicje:

1. **Administrator Danych** – Szkoła Podstawowa w Garbowie, reprezentowana przez Dyrektora.
2. **Analiza ryzyka** – proces dążący dookreślenia charakteru i poziomu ryzyka.
3. **Dane osobowe** – wszelkie 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.
4. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie.

5. **Inspektor Ochrony Danych** – osoba, którą wyznaczył Administrator Danych i powiadomił o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych.
6. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
7. **Naruszenie ochrony danych osobowych (incydent ochrony danych)**– 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.
8. **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 Europejskiej 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 co celów przetwarzania.
9. **Organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych.
10. **Osoba upoważniona** – osoba posiadająca formalne upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych lub osobą przez niego wyznaczoną.
11. **Podmiot przetwarzający (procesor)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane w imieniu Administratora Danych.
12. **Przetwarzanie** – operacja 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.
13. **System teleinformatyczny** – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. System ten tworzy sieć telekomunikacyjną Administratora Danych.
14. **Użytkownik** – osoba upoważniona do przetwarzania danych osobowych, której przyznano identyfikator i hasło.
15. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

16. **Zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
17. **Zarządzanie incydentami związanymi z bezpieczeństwem informacji** – procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji.
18. **Zarządzanie ryzykiem** – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka.

2. Osoby odpowiedzialne za bezpieczeństwo informacji i przetwarzanie danych osobowych:

2.1. Obowiązki Administratora Danych:

1) Wdraża odpowiednie środki organizacyjne i techniczne, aby przetwarzanie danych odbywało się zgodnie z prawem, z uwzględnieniem charakteru, kontekstu, zakresu i celu przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze. Analiza ryzyka stanowi załącznik nr 2 do niniejszej Polityki.
2) Podejmuje decyzje o celach i środkach przetwarzania danych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji i technik zabezpieczania danych.
3) Upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym zakresie, odpowiadającym zakresowi jej obowiązków.
4) Powołuje Inspektora Ochrony Danych w oparciu o art. 37 RODO, o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia jego wyznaczenia. Zmiana danych Inspektora bądź jego odwołanie następuje z zachowaniem ww. terminu. Administrator Danych udostępnia na swojej stronie internetowej dane kontaktowe Inspektora tj.: imię nazwisko, nr telefonu lub adres e-mail.
5) Prowadzi rejestr czynności przetwarzania zgodnie z art. 30 RODO, który stanowi załącznik nr 3 do niniejszej Polityki. Administrator Danych może zlecić prowadzenie przedmiotowego rejestru Inspektorowi Ochrony Danych.
6) Dokonuje oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania w przypadku, gdy istnienie duże prawdopodobieństwo, że dany rodzaj przetwarzania powodować będzie wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
7) Zgłasza naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamiania o tym osoby, których te dane dotyczą.

2.2.Rola Inspektora Ochrony Danych:

Inspektor Ochrony Danych pełni funkcję opiniodawczo-doradczo-weryfikacyjną oraz odpowiedzialny jest w szczególności za:

1) Informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych osobowych i doradzanie im w tej sprawie.
2) Monitorowanie przestrzegania RODO, innych aktów unijnych lub państw członkowskich, o ochronie danych osobowych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania danych osobowych oraz powiązane z tym audyty.
3) Udzielanie na żądanie zaleceń do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania.
4) Współpracę z organem nadzorczym.
5) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.
6) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z uprzednimi konsultacjami, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach.
7) Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia o Ochronie Danych Osobowych.
8) Prowadzenie rejestru czynności na polecenie Administratora Danych.

2.3.Obowiązki osoby zajmującej się obsługą informatyczną Jednostki:

Osoba ta odpowiedzialna jest za zarządzanie i bieżący nadzór nad systemem informatycznym Administratora Danych, w tym:

1) Przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta użytkowników zgodnie z zapisami niniejszego dokumentu.
2) Resetuje hasła dostępu na poszczególnych stacjach, ujawniając je wyłącznie danemu użytkownikowi.

3) W sytuacji naruszenia zabezpieczeń systemu informatycznego informuje Inspektora Ochrony Danych i współdziała przy usuwaniu skutków naruszenia.
4) Sprawuje nadzór nad wykonywaniem: napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii sytemu informatycznego.
5) Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.
6) Prowadzi ewidencję oraz inwentaryzuje sprzęt komputerowy i oprogramowanie.

3. Podstawy przetwarzania danych osobowych:

Szkoła Podstawowa w Garbowie działa wyłącznie w granicach określonych przepisami prawa i przetwarza dane osobowe osób fizycznych głównie w oparciu o przesłanki określone w art. 6 Rozporządzenia 2016/679. Mając na uwadze powyższe, przetwarzanie danych dopuszczalne jest w sytuacji, gdy:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych osobowych w jednym lub większej liczbie określonych celów,
2) przetwarzanie jest niezbędne do wykonania umowy, gdzie stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy,
3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
4) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,
5) przetwarzanie jest niezbędne do wykonania zadań realizowanych w interesie publicznym lub do sprawowania władzy publicznej powierzonej Administratorowi.

4. Obowiązek informacyjny:

Administrator Danych podczas pozyskiwania danych od osoby, której dane dotyczą jest zobowiązany poinformować tę osobę o:

1) Swojej tożsamości i danych kontaktowych,
2) Danych kontaktowych Inspektora Ochrony Danych,
3) Celu i podstawie prawnej przetwarzania tych danych osobowych,
4) Prawnie uzasadnionym interesie realizowanym przez Administratora Danych lub stronę trzecią,
5) Odbiorcach danych lub kategorii odbiorców,

6) Okresie, przez który te dane będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia takiego okresu,
7) Prawie do żądania od Administratora:
    a) dostępu do danych osobowych osoby, której te dane dotyczą,
    b) do sprostowania jej danych osobowych,
    c) do usunięcia jej danych osobowych,
    d) do ograniczenia przetwarzania jej danych osobowych,
    e) do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych,
    f) do przenoszenia danych;
8) Prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem - jeżeli przetwarzanie odbywa się na podstawie zgody,
9) Prawie wniesienia skargi do organu nadzorczego,
10) Właściwości: czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do ich podania i jakie są ewentualne konsekwencje nie podania tych danych,
11) Zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
12) Zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,
13) W przypadku zbierania danych nie od osoby, której dane dotyczą, osobę tę należy poinformować dodatkowo o kategorii i źródle pochodzenia danych osobowych.

5. Prawa osoby, której dane dotyczą:

Osoba, której dane dotyczą ma prawo:

a) żądania od Administratora dostępu do swoich danych,
b) do sprostowania swoich danych,
c) do usunięcia swoich danych,
d) do ograniczenia przetwarzania swoich danych,
e) do wniesienia sprzeciwu do przetwarzania swoich danych,

f) do przenoszenia danych.

Każda osoba, której dane dotyczą, ma prawo skorzystać z niniejszych praw poprzez złożenie wniosku do Szkoły Podstawowej w Garbowie. Przedmiotowy wniosek zostaje dekretowany do Administratora Danych, który analizuje treść dokumentu. Następnie wniosek przesłany zostaje Inspektorowi Danych Osobowych do analizy, po której sporządza on notatkę i w formie pisemnej przesyła wraz z przedmiotowym wnioskiem propozycję wykonania czynności Administratorowi Danych. Administrator Danych po weryfikacji przedstawionych dokumentów kieruje wniosek do wyznaczonego pracownika merytorycznego udzielając mu zaleceń dotyczących przygotowania treści dokumentu celem udzielenia odpowiedzi wnioskodawcy.

6. Udostępnianie danych osobowych:

Administrator Danych udostępnia przetwarzane dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na podstawie i w granicach przepisów prawa tj.:

a) na wniosek osoby, której dane dotyczą,
b) za wyraźną zgodą podmiotu, którego dane dotyczą,
c) na wniosek podmiotu uprawnionego do otrzymywania danych osobowych (np.: Policji, Prokuraturze),
d) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych.

Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystywać wyłącznie w celu, dla którego zostały zebrane.

W przypadku wpływu wniosku pochodzącego od osoby, której dane dotyczą w sprawie żądania udzielenia informacji na temat przetwarzania jej danych osobowych, odpowiedź na przedmiotowy wniosek następuje w terminie 30 dni od daty jego otrzymania.

7. Bezpieczeństwo fizyczne jednostki

Budynek jednostki zabezpieczony został alarmem antywłamaniowym, do którego kod znają jedynie uprawnieni pracownicy. Ponadto budynek podlega również całodobowej ochronie poprzez zastosowanie zabezpieczenia w postaci monitoringu wizyjnego. Obszar, który został poddany rejestracji obrazu oznakowany jest stosownymi tablicami informującymi o funkcjonowaniu monitoringu. Kamery monitorujące umieszczone są w miejscach, w których obraz nie narusza godności człowieka oraz jego prawa do prywatności, w szczególności poza pomieszczeniami:

a) w których odbywają się zajęcia dydaktyczne, wychowawcze, opiekuńcze;
b) w których udzielana jest pomoc psychologiczno-pedagogiczna uczniom;

c) przeznaczone do odpoczynku i rekreacji pracowników;

d) sanitarnohigienicznymi gabinetem profilaktyki zdrowotnej, szatnie, przebieralnie.

Celem zainstalowania monitoringu wizyjnego jest zapewnienie bezpieczeństwa uczniów i pracowników oraz/lub ochrona mienia. Rejestrator monitoringu znajduje się w gabinecie dyrektora szkoły. Dostęp do zapisu posiada Administrator Danych, a także osoby przez niego upoważnione. Rejestracji oraz zapisywaniu na nośniku fizycznym podlega wyłącznie obraz (wizja) z kamer systemu, dźwięk natomiast nie jest rejestrowany. Materiał archiwalny przechowywany jest przez okres 30 dni od daty nagrania od dnia nagrania, a następnie usuwany poprzez nadpisanie. Regulamin monitoringu został uregulowany Zarządzeniem 4-2018/2019 z dnia 25.03.2019r..

8. Zasady bezpieczeństwa na stanowisku pracy

Każdy pracownik w chwili rozpoczęcia pracy zobowiązany jest do zwrócenia szczególnej uwagi na stan zabezpieczenia pomieszczenia (drzwi, okna), stan szaf, biurek i urządzeń pozostających w eksploatacji użytkownika. W przypadku pracy na stacji roboczej włączenie i logowanie do komputera powinno jednocześnie stanowić kontrolę tego kto był ostatnim logującym się użytkownikiem. W przypadku stwierdzenia jakichkolwiek nieprawidłowości pracownik powiadamia swoich przełożonych. Ponadto każdy pracownik zobowiązany jest także do przestrzegania opisanych poniżej zasad.

1) Zasada czystego ekranu

W przypadku każdorazowego opuszczenia stanowiska pracy, pracownik zobowiązany jest wylogować się z systemu lub zablokować dostęp do pulpitu stacji roboczej, w celu uniemożliwienia dostępu do systemu operacyjnego osób nieuprawnionych. Ponadto w trakcie pracy pracownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych, natomiast ekrany monitorów powinny być tak ustawione, aby osoby postronne nie miały możliwości wglądu w dane znajdujące się na monitorze.

2) Zasada czystego biurka

Każdy pracownik w trakcie pracy powinien mieć na biurku tylko i wyłącznie te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu pracy pracownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających dane, w celu uniemożliwienia dostępu osób nieuprawnionych.

3) Zasada czystego kosza

Dokumenty w formie papierowej, z wyjątkiem materiałów promocyjnych, marketingowych oraz informacyjnych powinny być niszczone w sposób uniemożliwiający ich ponowne odczytanie, poprzez zniszczenie w niszczarce bądź umieszczenie w specjalnych pojemnikach. Niedozwolone jest natomiast wyrzucenie dokumentów do kosza na śmieci.

4) Zasada zamkniętego pomieszczenia

Opuszczając pomieszczenie służbowe, pracownik zobowiązany jest je zabezpieczyć zarówno w godzinach pracy, jak i po jej zakończeniu, jeżeli nie pozostaje w nim inna osoba upoważniona. Zasada ta nie dotyczy pomieszczeń ogólnodostępnych np. sale. Po zakończeniu pracy ostatnia wychodząca z pomieszczenia osoba, zamyka wszystkie drzwi i deponuje klucze na portierni.

9. Zasady dokonywania anonimizacji danych osobowych publikowanych powszechnie, w tym w Biuletynie Informacji Publicznej oraz na stronach internetowych:

Pracownik odpowiedzialny za sporządzenie dokumentów, które mają zostać zamieszczone w Biuletynie Informacji Publicznej i/lub na stronach internetowych zobowiązany jest do wstępnej oceny przedmiotowego dokumentu pod względem dopuszczalności publikacji danych osobowych osób fizycznych, które nie pełnią funkcji publicznych/kierowniczych. W przypadku, gdy wstępna ocena wykaże obecność występowania danych osobowych osób fizycznych pracownik ten zobowiązany jest do dokonania analizy legalności publikacji danych osobowych w przedmiotowym dokumencie, a następnie anonimizacji zawartych w nim danych osobowych osób fizycznych tj. imion, nazwisk, adresu, stanu zdrowia, nr PESEL itp. (zgodnie z art. 6, 9, 10 RODO). Natomiast pracownik odpowiedzialny za publikację przedmiotowych dokumentów w Biuletynie Informacji Publicznej i/lub na stronach internetowych zobowiązany jest do sprawdzenia poprawności dokonanej anonimizacji danych osobowych w tych dokumentach.

10. Upoważnienie do przetwarzania danych osobowych oraz ewidencja osób upoważnionych:

Do przetwarzania danych osobowych mogą mieć dostęp wyłącznie osoby posiadające pisemne upoważnienie nadane przez Administratora Danych. Upoważnienie, wydawane jest na czas określony lub nieokreślony. Ponadto Administrator Danych zobowiązany jest wydać nowe lub cofnąć upoważnienie w przypadku zmiany stanowiska, zakresu obowiązków pracowniczych, przyjęcia do pracy nowej osoby lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzania danych osobowych. Za przygotowanie upoważnienia, którego wzór stanowi załącznik nr 4 do niniejszej Polityki odpowiedzialny jest samodzielny referentem szkoły ds. administracyjnych .

Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez osobę wyznaczoną, a jej wzór stanowi załącznik nr 5 do Polityki.

11. Umowy powierzenia przetwarzania danych osobowych:

Administrator Danych zawiera umowę powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym, który dokonuje przetwarzania danych osobowych w imieniu Administratora. Wszelkie postanowienia, którym powinna odpowiadać ww. umowa zostały zawarte w art. 28 RODO.

Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 14 do niniejszej Polityki.

12. Procedura zarządzania incydentami:

Zgodnie z art. 4 ust 12 RODO incydent ochrony danych stanowi naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W związku z powyższym każdy z pracowników ma obowiązek zgłaszać niezwłocznie wszelkie zauważone przez siebie naruszenia bezpieczeństwa informacji Administratorowi Danych Osobowych lub Inspektorowi Ochrony Danych. Ponadto zgłaszający zdarzenie nie powinien podejmować żadnych działań na własną rękę, jednakże w miarę możliwości powinien zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. Kwalifikacji czy zdarzenie wypełnia definicję naruszenia ochrony danych osobowych dokonuje Administrator Danych Osobowych oraz Inspektor Ochrony Danych biorąc pod uwagę identyfikację zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie jako:

a) zdarzenie, które nie posiada cech naruszenia bezpieczeństwa informacji, np.: przerwa w dostawie prądu,
b) błąd w działaniu elementu infrastruktury teleinformatycznej lub infrastruktury biurowej,
c) awaria techniczna, która czasowo blokuje dostęp do informacji,
d) incydent związany z naruszeniem integralności, dostępności, poufności.

W przypadku stwierdzenia wystąpienia incydentu Administrator Danych Osobowych oraz Inspektor Ochrony Danych prowadzą postępowanie wyjaśniające, w którym:

a) ustala się rodzaj incydentu i miejsce wystąpienia,
b) ustala się zakres i przyczyny incydentu oraz jego ewentualne skutki,
c) podejmuje się działania na rzecz przywrócenia funkcjonowania organizacji po wystąpieniu incydentu,

d) rekomenduje się działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

Z przeprowadzonego postępowania zostaje sporządzony raport, którego wzór stanowi załącznik nr 6 do Polityki. Ponadto Administrator danych dokumentuje wszelkie naruszenia i okoliczności naruszenia ochrony danych w tym danych osobowych, jego skutki oraz podjęte działania zaradcze w rejestrze incydentów, którego wzór stanowi tabela zamieszczona w załączniku nr 6 do Polityki. W przypadku zakwalifikowania zdarzenia jako incydentu naruszenia ochrony danych Administrator Danych, bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenie, o którym mowa powyżej powinno zawierać co najmniej:

a) opis charakteru 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.

Jeżeli powyższych informacji nie można udzielić w tym samym czasie, można je udzielać sukcesywnie, lecz bez zbędnej zwłoki. W przypadku, gdy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych Administrator bez zbędnej zwłoki zawiadamia także osobę, której te dane dotyczą. Opisywane zawiadomienie powinno zawierać:

a) charakter naruszenia,
b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
c) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
d) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wskazane powyżej zawiadomienie nie jest wymagane, jeżeli:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony a środki te zostały zastosowane do danych w tym danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane.

13. Procedura retencji danych:

1) Poprzez retencję danych rozumie się ustalenie celu oraz okresu przechowywania zebranych danych osobowych.
2) Pracownik merytoryczny, który przetwarza dane osobowe zobowiązany jest:
    a) dokonać inwentaryzacji przetwarzanych danych osobowych w konkretnych procesach,
    b) sprawdzić miejsce przechowywania danych,
    c) sprawdzić formę przetwarzania danych,
    d) określić cel, dla którego dane zostały zebrane,
    e) określić czas przechowywania danych poprzez analizę przepisów szczegółowych, z których wynika okres przechowywania danych, a jeżeli taki okres nie jest podany, ustalić kryteria ustalenia okresu.
3) Ustalając okres retencji należy wziąć pod uwagę obecną i przyszłą wartość informacji, koszty, ryzyko i zobowiązania związane z przetwarzanie danych, a także realną możliwość zapewnienia, by dane były aktualne.
4) Po ustaniu okresu przechowywania, dane podlegają usunięciu, gdy:
    a) minął okres ich przydatności,
    b) okaże się, że cel, dla którego dane zostały zebrane został osiągnięty.

14. Szczegółowe wytyczne organizacyjne zawierające w/w procedury stanowią załączniki do Polityki Ochrony Danych Osobowych:

- Zał. nr 1 Oświadczenie o znajomości Polityki Ochrony Danych Osobowych oraz zachowaniu poufności.
- Zał. nr 2 Analiza ryzyka.

- Zał. nr 3 Rejestr czynności przetwarzania danych osobowych.
- Zał. nr 4 Upoważnienie do przetwarzania danych osobowych.
- Zał. nr 5 Ewidencja osób upoważnionych.
- Zał. nr 6 Raport z naruszenia ochrony danych osobowych.
- Zał. nr 7 Polityka kluczy.
- Zał. nr 8 Procedura nadawania i rejestrowania uprawnień.
- Zał. nr 9 Wniosek o nadanie uprawnień.
- Zał. nr 10 Karta ewidencyjna uprawnień użytkownika.
- Zał. nr 11 Zasady konserwacji i serwisowania sprzętu zawierającego dane osobowe.
- Zał. nr 12 Ogólne procedury użytkowania i zabezpieczeń infrastruktury IT.
- Zał. nr 13 Zasady wykorzystania systemu teleinformatycznego.
- Zał. nr 14 Wzór umowy powierzenia danych osobowych.
- Zał. nr 15 Zgoda na wykorzystanie wizerunku.