……

Polityka ochrony danych osobowych

Zatwierdził:

31.08.2018 r. Beata Czapla

(data, podpis)

Niniejszy dokument jest Polityką Ochrony Danych Osobowych w rozumieniu RODO – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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. Urz. UE L 119, s.1).

Zawiera on:

a) opis zasad ochrony danych obowiązujących w Szkole Podstawowej nr 10 im. Stefana Żeromskiego w Koszalinie.
b) odwołania do procedur i instrukcji dotyczących poszczególnych obszarów ochrony danych osobowych.

Polityka Ochrony Danych Osobowych została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymaganiami RODO.

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Dyrektor Szkoły. Za nadzór i monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych. Do stosowania Polityki zobowiązani są wszyscy pracownicy przetwarzający dane osobowe.

§ 1 Skróty i definicje

Stosowane w niniejszym dokumencie skróty i definicje oznaczają:

a) Polityka oznacza niniejszą Politykę bezpieczeństwa, o ile co innego nie wynika wyraźnie z kontekstu,
b) RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1),
c) Dane osobowe oznaczają wszystkie informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych,
d) Dane wrażliwe oznaczają dane specjalne i dane karne,
e) Dane specjalne oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
f) Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa,
g) Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu,
h) Podmiot przetwarzający oznacza organizację lub osobę, której Szkoła powierzyła przetwarzanie danych osobowych (np. usługodawca IT),
i) Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
j) Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej,
k) IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych,
l) RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych,

m) Administrator Danych oznacza Szkołę Podstawową nr 10 im. Stefana Żeromskiego w Koszalinie.

§ 2 Inspektor Ochrony Danych

1. Administrator Danych jest podmiotem publicznym, który na mocy art. 37 ust. 1 RODO ma obowiązek powołania Inspektora Ochrony Danych (IOD).

2. Osoba powołana na stanowisko IOD posiada:
   a) odpowiednią wiedzę fachową tj. gruntowną wiedzę na temat krajowego i europejskiego prawa oraz praktyk w dziedzinie ochrony danych osobowych,
   b) znajomość struktury administratora oraz wiedzę o dokonywanych czynnościach przetwarzania a także o systemach informatycznych oraz o potrzebach administratora w zakresie bezpieczeństwa i ochrony danych,
   c) znajomość przepisów administracyjnych oraz postępowania administracyjnego w jednostce organizacyjnej,

   i odpowiednie cechy osobowe tj. uczciwość i wysoko rozwiniętą etykę zawodową.

3. IOD jest zatrudniony na podstawie umowy cywilno-prawnej i został powołany dokumentem „Wyznaczenie Inspektora Ochrony Danych".

4. IOD podlega bezpośrednio Dyrektorowi Szkoły.

5. IOD wykonuje obowiązki wskazane w art. 39 RODO.

§ 3 Zasady ochrony przetwarzania danych osobowych

Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem,
2. rzetelnie i uczciwie,
3. w sposób przejrzysty dla osoby, której dane dotyczą,
4. w konkretnych celach,
5. tylko niezbędne dane,
6. nie dłużej niż trzeba,
7. zapewniając odpowiednie bezpieczeństwo danych.

§ 4 System ochrony danych

Na system ochrony danych osobowych składają się następujące elementy:

1. zidentyfikowane zbiory danych osobowych oraz opis sposobów ich przetwarzania,
2. Rejestr Czynności Przetwarzania Danych Osobowych,
3. podstawy prawne przetwarzania danych osobowych,
4. zasady realizacji obowiązku informacyjnego,
5. procedury obsługi praw osób, których dane są przetwarzane,
6. metody zarządzania minimalizacją przetwarzanych danych,
7. procedury zapewniające odpowiedni poziom bezpieczeństwa danych,
8. zasady identyfikacji i obsługi incydentów,
9. procedura przywrócenia dostępności danych osobowych w razie wystąpienia incydentu,
10. zasady powierzania przetwarzania danych podmiotom zewnętrznym,

11. zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe.

4.1. Identyfikacja zbiorów danych osobowych

Administrator danych zidentyfikował procesy i zbiory, w których są przetwarzane dane osobowe. Dla każdego zbioru wskazano właściciela i zweryfikowano czy nie zachodzi przypadek współadministrowania. W ramach przeprowadzonej inwentaryzacji zostały wskazane grupy informacji przetwarzane w zbiorach. W ramach każdego zbioru dokonano analizy związanej z przetwarzaniem szczególnych kategorii danych osobowych oraz ewentualnym profilowaniem. W ramach inwentaryzacji wskazano również aplikacje, które służą do przetwarzania danych.

Zinwentaryzowane zbiory zostały opisane w „Wykazie zbiorów w których przetwarzane są dane osobowe", który zawiera informacje wskazane w załączniku nr 1 do niniejszej Polityki.

4.2. Rejestr Czynności Przetwarzania Danych Osobowych

Administrator danych prowadzi, zgodnie z wymaganiami art. 30 RODO, Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr stanowi formę dokumentowania czynności przetwarzania danych osobowych. Za prowadzenie Rejestru odpowiada IOD. Rejestr jest aktualizowany w przypadku podjęcia przez Administratora nowych czynności przetwarzania danych. Wzór Rejestru Czynności Przetwarzania Danych stanowi załączniku nr 2 do Polityki.

Niektóre dane osobowe są przetwarzane w podmiocie przetwarzającym na podstawie umowy powierzenia przetwarzania. Rejestr dla tych danych prowadzony jest zgodnie ze wzorem stanowiącym zał. nr 3 do Polityki.

4.3. Podstawy prawne przetwarzania danych osobowych

Administrator dokumentuje w Wykazie zbiorów, o którym mowa w pkt. 4.1. podstawy prawne przetwarzania danych osobowych dla poszczególnych zbiorów. W przypadku każdego zbioru wskazuje podstawę prawną przetwarzania danych zwykłych i szczególnych kategorii danych osobowych, które wynikają z RODO (np. zgoda, umowa czy obowiązek prawny) i dookreśla je dodatkowymi informacjami np. dla zgody wskazując na jej zakres a w przypadku podstawy prawnej konkretny przepis ustawy branżowej. Podstawy prawne są okresowo weryfikowane.

4.4. Zasady realizacji obowiązku informacyjnego

Przy pozyskiwaniu danych osobowych od osoby, której dane dotyczą Administrator spełnia obowiązek informacyjny opisany w art. 13 RODO.

W przypadku pozyskiwania danych od potencjalnych pracowników, Administrator przekazuje w ogłoszeniu o rozpoczęciu rekrutacji informację o miejscu publikacji klauzuli informacyjnej.

Przy zbieraniu danych od pracowników obowiązek informacyjny realizowany jest przez udostępnienie informacji o przetwarzaniu danych pracownika w formie dokumentu papierowego i potwierdzenie jej odebrania przez złożenie podpisu pod stosownym oświadczeniem. W stosunku do osób zatrudnionych u Administratora w dniu wejścia w życie niniejszej Polityki obowiązek informacyjny został zrealizowany przez udostępnienie klauzuli w formie papierowej i potwierdzenie podpisem zapoznania się z nią.

W przypadku pozyskiwania danych osobowych od rodziców (dane osobowe rodziców i uczniów), każdy z nich ma możliwość zapoznania się z odpowiednią klauzulą informacyjną wywieszoną na tablicy ogłoszeń w siedzibie administratora i opublikowaną w BIP-ie szkoły.

W innych przypadkach pozyskiwania danych osobowych, podmiotom danych jest udostępniana informacja o miejscu publikacji klauzuli informacyjnej.

Sposób realizacji obowiązku informacyjnego dla każdego zbioru jest wskazany w Wykazie zbiorów, o którym mowa powyżej.

4.5. Procedury obsługi praw osób, których dane są przetwarzane

W celu właściwej obsługi praw osób, których dane są przetwarzane przez Administratora, została opracowana Procedura obsługi żądań podmiotu danych, która stanowi załącznik nr 3 do Polityki.

4.6. Metody zarządzania minimalizacją przetwarzanych danych

Na minimalizację przetwarzania danych mają wpływ następujące czynniki:

- adekwatność danych w stosunku do celu przetwarzania,

- dostęp do danych tylko dla tych osób i w takim zakresie jak jest to niezbędne,

- przechowywanie danych nie dłużej niż jest to niezbędne.

W ramach wdrażania RODO Administrator zweryfikował zakres pozyskiwanych informacji oraz zakres ich przetwarzania pod kątem adekwatności w stosunku do celu. Administrator zobowiązał właścicieli danych osobowych do okresowego przeglądu pozyskiwanych i przetwarzanych danych osobowych, by zapewnić, że ich zakres nie wykracza ponad niezbędne minimum. W celu wywiązania się z tego zadania, właściciel danych powinien między innymi zweryfikować, czy nie nastąpiły zmiany w przepisach prawa.

W celu minimalizacji dostępu do danych osobowych Administrator stosuje ograniczenia organizacyjne, fizyczne i logiczne. Ograniczenia organizacyjne realizowane są poprzez odbieranie od pracowników zobowiązań o zachowaniu poufności i określanie zakresu upoważnień do przetwarzania danych. Ograniczenia fizyczne wynikają z reglamentacji dostępu do pomieszczeń i dokumentów. Ograniczenia logiczne realizowane są przez nadawanie odpowiednich uprawnień dostępowych do zasobów sieciowych i systemów, w których są przetwarzane dane osobowe. Uprawnienia dostępowe są aktualizowane przy zmianie stanowiska lub roli pracownika w procesie przetwarzania danych. Administrator zapewnia, że przynajmniej raz do roku dokonuje przeglądu użytkowników systemów i nadanych im uprawnień. Szczegółowe zasady zarządzania uprawnieniami zostały opisane w Procedurze nadawania i zmiany uprawnień.

Administrator zarządza cyklem życia dokumentów. Jednolity Rzeczowy Wykaz Akt / Instrukcja kancelaryjna określa zarówno okres przechowywania dokumentów na stanowisku pracy jak i okres ich archiwizacji. Administrator zapewnia, że dokumenty przechowywane w archiwum są poddawane okresowym przeglądom i że są niszczone w bezpieczny sposób po upływie okresu ich przechowywania.

4.7. Procedury zapewniające odpowiedni poziom bezpieczeństwa

Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych przez:

- zapewnienie odpowiedniego stanu wiedzy o bezpieczeństwie i zagrożeniach wynikających z przetwarzania danych osobowych (szkolenia pracowników),

- okresowe przeprowadzanie analizy ryzyka i dobór możliwych do zastosowania zabezpieczeń technicznych i organizacyjnych zgodnie z Procedurą analizy ryzyka załącznik nr 4 do Polityki,

- weryfikację skuteczności wdrożonych zabezpieczeń.

Administrator jest zwolniony z przeprowadzania oceny skutków dla ochrony danych dla tych operacji przetwarzania, które mają podstawę prawną w prawie polskim lub prawie UE.

Administrator dokonuje oceny skutków dla ochrony danych w tych operacjach, które wskazuje organ nadzorczy.

Po wdrożeniu nowych zabezpieczeń, ustanowionych w wyniku przeprowadzonej analizy ryzyka i ewentualnie oceny skutków dla ochrony danych osobowych administrator aktualizuje dokument Wykaz stosowanych zabezpieczeń.

4.8. Zasady identyfikacji i obsługi incydentów

Administrator przyjął zasady zobowiązujące wszystkich pracowników do powiadamiania o stwierdzeniu podatności systemu ochrony danych lub wystąpieniu incydentu bezpieczeństwa. Zasady te zostały opisane w Regulaminie ochrony danych osobowych.

Procedura obsługi naruszeń ochrony danych stanowi załącznik nr 5 do Polityki.

4.9. Zasady powierzania przetwarzania danych podmiotom zewnętrznym

Administrator opracował ankietę, na podstawie której weryfikuje nowe firmy, z którymi zamierza podpisać umowy powierzenia przetwarzania danych osobowych (załącznik nr 6 do Polityki). Weryfikacja firm ma zapewnić, że podmioty przetwarzające dają wystarczające gwarancje bezpiecznego przetwarzania danych osobowych.

Administrator opracował wzór umowy powierzenia przetwarzania danych osobowych, które stanowi załącznik nr 7 do Polityki.

Administrator prowadzi rejestr umów, na podstawie których powierzył przetwarzanie danych podmiotom zewnętrznym.

4.11. Zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe

W przypadku uruchamiania nowych projektów związanych z przetwarzaniem danych osobowych administrator zapewnia, że uwzględnia w nich zagadnienia związane z bezpieczeństwem i minimalizacją przetwarzanych danych.

§ 5 Postanowienia końcowe

1. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych jest przeszkolony w zakresie RODO i wewnętrznych regulacji dotyczących ochrony danych osobowych.
2. Zbiór podstawowych zasad bezpiecznego przetwarzania danych osobowych został zapisany w Regulaminie ochrony danych osobowych (załącznik nr 8 do Polityki).
3. Po zapoznaniu się z zasadami ochrony danych osobowych, pracownik potwierdza znajomość tych zasad i deklaruje ich stosowanie.

Politykę ochrony danych osobowych wprowadzono Zarządzeniem nr 36/2017/2018 Dyrektora Szkoły z dnia 31 sierpnia 2018 r.

Zał. nr 1 do Polityki

Wykaz zbiorów - Szkoła Podstawowa nr 10 im. Stefana Żeromskiego w Koszalinie

Numer zbioru	Nazwa zbioru	Nazwa systemu	Login
1	Rekrutacja uczniów	Nabór	x
2	Księga ewidencji dzieci (tylko szkoła obwodowa)		
3	Księga ewidencji uczniów	Sekretariat	x
4	Dziennik lekcyjny	eDziennik	x
5	Dziennik zajęć w świetlicy		
6	Dziennik innych zajęć, w tym z zakresu pomocy psychologiczno-pedagogicznej		
7	Dziennik zajęć rewalidacyjno-wychowawczych		
8	Dzienniki specjalistów (psychologa, pedagoga, logopedy)		
9	Indywidualna teczka ucznia (arkusz diagnozy IPET)		
10	Opinie i orzeczenia poradni psychologiczno-pedagogicznej		
11	Księga arkuszy ocen, arkusze ocen		
12	Upoważnienia do odbioru dziecka		
13	Ewidencja świadectw ukończenia szkoły i zaświadczeń z OKE		
14	Ewidencja legitymacji szkolnych		
15	Dokumentacja wypadków uczniów		
16	Akta osobowe pracowników	Kadry, SIO, Arkusz organizacyjny	x
17	Dokumentacja płacowa	Płace	x
18	Zgłoszenia do ZUS + zwolnienia lekarskie	Płatnik	x
19	Dokumentacja wypadków pracowników		
20	Zapomogi zdrowotne		
21	ZFŚS, komisja socjalna		
22	Monitoring szkolny		
23	Rejestr korespondencji przychodzącej i wychodzącej	PROTON	x
24	Kontrahenci	Finanse	x
25	zamówienia publiczne		

Zał. nr 2 do Polityki

Rejestr Czynności Przetwarzania

Nazwa zbioru / procesu	
Cele przetwarzania	
Kategorie osób, których dane dotyczą	
Kategorie danych osobowych	
Kategorie odbiorców	
Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
Nazwa państwa trzeciego lub w organizacji międzynarodowej, do których następuje transfer (dokumentacja zabezpieczeń transferu)	
Planowane terminy usunięcia danych	
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	

Zał. nr 3 do Polityki

PROCEDURA OBSŁUGI ŻADAŃ PODMIOTU DANYCH

Procedura opisuje sposób postępowania Administratora danych w sytuacji, gdy osoba, której dane dotyczą skieruje do Administratora danych żądanie związane z realizacją jej praw, określonych w art. 15 – 18 i 20 - 21 RODO.

Żądanie związane z realizacją praw podmiotu danych może wpłynąć do Administratora danych w formie:
- tradycyjnej (papierowej) – na adres korespondencyjny,
- elektronicznej – na dedykowany adres IOD, adres sekretariatu lub dowolnej komórki organizacyjnej,
- ustnej – kierowanej do pracowników Administratora danych.

RODO nie precyzuje treści żądania. Każde żądanie, które wpłynęło do Administratora danych, niezależnie od formy, powinno trafić do IOD w celu jego zaewidencjonowania i rozpatrzenia. Rozpatrywanie żądań powinno być realizowane w oparciu o schematy postępowania, które stanowią załączniki do niniejszej procedury.

Gdy Administrator uzna, że żądania wnioskodawcy są ewidentnie nieuzasadnione bądź nadmierne, to może, działając zgodnie z art. 12 ust. 5 RODO:
- pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, lub
- odmówić podjęcia działań w związku z żądaniem.
Na Administratorze ciąży wtedy obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter.

Działania niezbędne do rozpatrzenia i realizacji żądania wykonuje IOD przy wsparciu osób wskazanych przez Administratora danych. Propozycję odpowiedzi na żądanie dotyczące realizacji praw podmiotu danych zespół każdorazowo przedstawia Administratorowi do akceptacji. Wszystkie odpowiedzi są archiwizowane przez IOD.

Odpowiedź powinna być udzielona niezwłocznie, nie później niż w ciągu 30 dni od otrzymania żądania.

IOD zobowiązany jest do wykorzystania dostępnych środków w celu zweryfikowania tożsamości osoby zwracającej się z żądaniami dotyczącymi realizacji jej praw, zwłaszcza gdy żądanie skierowane było drogą elektroniczną.

Realizacja żądania na podstawie art. 15 RODO

Prawo dostępu do danych osobowych

1. Wniosek o udzielenie informacji

Z wnioskiem do Administratora danych o udzielenie informacji na temat przetwarzania danych osobowych może się zwrócić każda osoba, niezależnie od tego, czy Administrator takie dane przetwarza czy też nie.

Odpowiedź twierdząca Administratora danych może stanowić podstawę do realizacji praw wynikających z art. 16 – 18 i 20 - 21.

2. Sprawdzenie czy Administrator danych przetwarza dane osobowe wnioskodawcy

Administrator danych sprawdza, czy na jakimkolwiek etapie przetwarza dane osobowe wnioskodawcy (między innymi czy dane przechowuje w Zakładowej Składnicy Akt). Sprawdzeniu podlegają zarówno zbiory prowadzone w wersji papierowej jak i elektronicznej. W przypadku, gdy Administrator danych nie przetwarza danych osobowych wnioskodawcy, powinien o tym wnioskodawcę poinformować.

3. Sprawdzenie czy przepisy szczególne wyłączają obowiązek informacyjny

Obowiązek informacyjny może podlegać ograniczeniom wynikającym z przepisów szczególnych. Między innymi w art. 6 projektu Ustawy o ochronie danych osobowych przewidziane są wyjątki dotyczące realizacji obowiązku informacyjnego przez organy publiczne. Jeżeli taka sytuacja ma miejsce Administrator danych odmawia udzielenia informacji wskazując przepisy ustaw szczególnych, które wyłączają obowiązek informacyjny.

4. Wezwanie do udzielenia dodatkowych informacji

Art. 6 ust. 2 projektu Ustawy o ochronie danych osobowych, w przypadku wykonywania zadań publicznych, daje możliwość wezwania wnioskodawcy do udzielenia dodatkowych informacji pozwalających na wyszukanie danych osobowych. Dalsze kroki procedury realizowane będą po uszczegółowieniu wniosku.

5. Ocena czy żądania są ewidentnie nieuzasadnione lub nadmierne

Jeżeli Administrator danych stwierdzi, że żądania wnioskodawcy są ewidentnie nieuzasadnione lub nadmierne (musi to wykazać), to ma prawo skorzystać z art. 12 ust. 5 RODO i może pobrać rozsądną opłatę lub odmówić podjęcia działań w związku z żądaniem. W obu przypadkach Administrator danych powinien uwzględnić okoliczności faktyczne i rozważyć konsekwencje dokonania wyboru.

W przypadku odmowy podjęcia działań Administrator danych informuje o tym fakcie wnioskodawcę.

W przypadku skorzystania z możliwości pobrania rozsądnej opłaty Administrator wzywa wnioskodawcę do jej uiszczenia i dopiero po jej otrzymaniu podejmuje dalsze kroki.

6. Udzielenie informacji

Administrator danych potwierdza przetwarzanie danych wnioskodawcy i przygotowuje odpowiedź, która zawiera informacje opisane w art. 15 RODO.

Odpowiedź powinna być przekazana w taki sam sposób w jaki wpłynęło żądanie.

Realizacja żądania na podstawie art. 16 RODO

Prawo dostępu do danych osobowych

1. Wniosek o sprostowanie (skorygowanie, uzupełnienie) danych osobowych

Jeżeli osoba, której dane dotyczą, na podstawie uzyskanych od administratora informacji stwierdzi, że dane na jej temat są nieprawidłowe (nieaktualne, błędne, niekompletne), to może się zwrócić do Administratora danych z żądaniem ich sprostowania lub uzupełnienia. Podmiot danych musi okazać dokument potwierdzający prawidłowe i aktualne dane lub w inny sposób wykazać swoje roszczenia.

2. Sprawdzenie czy spełnienie żądania regulowane jest przepisami szczególnymi i czy jest zasadne

Administrator danych sprawdza, czy sprostowanie danych jest regulowane w obowiązujących go przepisach szczególnych. Na przykład oczywiste pomyłki w decyzjach administracyjnych prostuje organ, który je uczynił w drodze postanowienia, na które przysługuje zażalenie.
W w/w przypadku nie można się powołać na przepisy RODO. Osobną kwestią pozostaje sprawdzenie, czy żądanie jest zasadne. Przy rozpatrywaniu zasadności wniosku, związanego z niekompletnością danych należy brać pod uwagę cele przetwarzania. Jeżeli zachodzi któraś z wymienionych przesłanek (sprostowanie danych regulują inne przepisy, żądanie jest nieuzasadnione) Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Spełnienie żądania

Jeżeli żądanie jest zasadne Administrator powinien je zrealizować i poinformować wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące w przypadku, kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

W przypadku, gdy Administrator danych udostępnił dane odbiorcy, powinien poinformować odbiorcę o dokonanym sprostowaniu danych, chyba że będzie to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Realizacja żądania na podstawie art.17 RODO

Prawo do usunięcia danych osobowych („Prawo do bycia zapomnianym")

1. Wniosek o usunięcie danych osobowych

Jeżeli osoba, której dane dotyczą:
- stwierdzi, że dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,

- cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
- wnosi sprzeciw wobec przetwarzania jej danych,
- stwierdzi, że dane osobowe były przetwarzane niezgodnie z prawem,
- stwierdzi, że dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator,
- stwierdzi, że dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego tzw. usług internetowych,
to może żądać od Administratora danych ich usunięcia. Wnioskodawca musi wykazać nieprawidłowości, nielegalność przetwarzania lub zbędność danych.

2. Sprawdzenie czy spełnienie żądania jest zasadne

Administrator danych sprawdza, czy zachodzi któraś z przesłanek wskazanych w art. 17 ust. 1 RODO, która uprawnia do wniesienia żądania. Jeżeli, w ocenie Administratora danych, nie zachodzi żadna z przesłanek pozwalających na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

3. Sprawdzenie czy nie zachodzą przesłanki wyłączające zapisy art. 17 ust. 1 i 2 RODO

Administrator danych sprawdza, czy można wykazać, że przetwarzanie danych jest niezbędne:
- do korzystania z prawa do wolności wypowiedzi i informacji (prawo wolności wypowiedzi i informacji ma prymat w stosunku do RODO),
- do wywiązania się z prawnego obowiązku lub wykonania zadania realizowanego w interesie publicznym bądź w ramach sprawowania władzy publicznej (przesłanka może być wykorzystywana w przypadku Administratorów danych z sektora publicznego),
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
- do celów archiwalnych, badań naukowych, historycznych lub statystycznych,
- do ustalenia, dochodzenia lub obrony roszczeń.
Jeżeli zachodzi któraś z wyżej wymienionych przesłanek wyłączających Prawo do usunięcia danych osobowych, to Administrator danych informuje wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych usuwa kwestionowane dane i informuje wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

W przypadku, gdy Administrator danych upublicznił dane osobowe, to uwzględniając dostępną technologię i koszty realizacji, podejmuje on rozsądne działania, by poinformować

administratorów przetwarzających te dane osobowe, że podmiot danych żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, ich kopie i replikacje.

Realizacja żądania na podstawie art.18 RODO

Prawo do ograniczenia przetwarzania

1. Wniosek o ograniczenie przetwarzania danych osobowych

Jeżeli osoba, której dane dotyczą kwestionuje prawidłowość danych, może zwrócić się do Administratora z żądaniem ograniczenia przetwarzania danych na okres pozwalający administratorowi sprawdzić prawidłowość tych danych.
Żądanie takie podmiot danych może skierować do administratora również w przypadku, gdy:
- przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
- administrator nie potrzebuje już danych osobowych do realizacji celu przetwarzania, ale są one potrzebne osobie, której dane dotyczą , do ustalenia, dochodzenia lub obrony roszczeń,
- osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania na mocy art., 21 ust. 1 RODO – do czasu stwierdzenia, czy prawnie uzasadnione podstawy prawne po stronie administratora są nadrzędne wobec podstaw prawnych sprzeciwu osoby, której dane dotyczą.

2. Sprawdzenie czy uprawnienie do żądania do ograniczenia przetwarzania zostało wyłączone na mocy przepisów szczególnych

Administrator danych sprawdza, czy ograniczenie przetwarzania danych jest regulowane w obowiązujących go przepisach szczególnych. W związku z wejściem RODO przewiduje się zmiany w dużej grupie przepisów szczególnych. Niektóre z nich będą wprowadzały wyłączenia wobec stosowania omawianego przepisu.

Jeżeli przepisy szczególne wprowadzają ograniczenia, to Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Sprawdzenie czy spełnienie żądania jest zasadne

Administrator danych sprawdza, czy zachodzi któraś z przesłanek wskazanych w art. 18 ust. 1 RODO, która uprawnia do wniesienia żądania. Jeżeli, w ocenie Administratora danych, nie zachodzi żadna z przesłanek pozwalających na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych je spełnia. Spełnienie żądania ograniczenia przetwarzania oznacza, że Administrator oznacza dane osobowe i przetwarzanie ogranicza do przechowywania. Administrator może przetwarzać dane w inny sposób wyłącznie za zgodą osoby której dane dotyczą albo w celu ustalenia, dochodzenia lub

obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Po spełnieniu żądania Administrator informuje wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

W przypadku, gdy Administrator danych udostępnił dane osobowe odbiorcy, to powinien poinformować odbiorcę, któremu ujawniono dane, o ograniczeniu przetwarzania danych, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Realizacja żądania na podstawie art.20 RODO

Prawo do przenoszenia danych

1. Wniosek o przeniesienie danych osobowych

Prawo do przeniesienia danych osobowych ma ułatwić zmianę dostawcy usług.
Żądanie przeniesienia danych osobowych podmiot danych może skierować do Administratora danych jeżeli przetwarzanie realizowane jest na podstawie zgody osoby, której dane dotyczą lub umowy oraz gdy przetwarzanie odbywa się w sposób zautomatyzowany. Celem realizacji żądania jest zmiana dostawcy usług.

2. Sprawdzenie czy uprawnienie do żądania do przeniesienia danych zostało wyłączone na mocy przepisów szczególnych

Administrator danych sprawdza, czy prawo do przenoszenia danych jest regulowane w obowiązujących go przepisach szczególnych. W związku z wejściem RODO przewiduje się zmiany w dużej grupie przepisów szczególnych. Niektóre z nich będą wprowadzały wyłączenia wobec stosowania omawianego przepisu.

Jeżeli przepisy szczególne wprowadzają ograniczenia, to Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Sprawdzenie czy spełnienie żądania jest zasadne

Administrator danych sprawdza, czy zachodzą przesłanki wskazane w art. 20 ust. 1 RODO, które uprawniają do wniesienia żądania. Jeżeli, w ocenie Administratora danych, nie zachodzą przesłanki pozwalające na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych je spełnia. Spełnienie żądania przeniesienia danych oznacza, że Administrator przekazuje dane osobowe, które otrzymał od podmiotu danych, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego osobie, której dane dotyczą lub innemu administratorowi, w zależności od żądania.

O realizacji żądania Administrator informuje wnioskodawcę. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

Realizacja żądania na podstawie art.21 RODO

Prawo wniesienia sprzeciwu

1. Wniesienie sprzeciwu

Jeżeli osoba, której dane dotyczą, sprzeciwia się przetwarzaniu danych osobowych, może wnieść do Administratora sprzeciw.
Sprzeciw nie przysługuje, gdy:
- przetwarzanie danych osobowych odbywa się na podstawie zgody na przetwarzanie (w tym wypadku osoba powinna cofnąć zgodę),
- podstawą przetwarzania danych osobowych jest konieczność realizacji umowy,
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

2. Sprawdzenie czy uprawnienie do wniesienia sprzeciwu zostało wyłączone na mocy przepisów szczególnych

Administrator danych sprawdza, czy ograniczenie wniesienie sprzeciwu jest regulowane w obowiązujących go przepisach szczególnych. W związku z wejściem RODO przewiduje się zmiany w dużej grupie przepisów szczególnych. Niektóre z nich będą wprowadzały wyłączenia wobec stosowania omawianego przepisu.

Jeżeli przepisy szczególne wprowadzają ograniczenia, to Administrator danych odmawia spełnienia żądania o czym informuje wnioskodawcę.

3. Sprawdzenie czy spełnienie żądania jest zasadne na podstawie art. 21 ust. 1

Administrator danych sprawdza, czy żądanie wynika z przesłanek wymienionych w art. 21 ust. 1 i czy zachodzi któraś z nich, tj.:

- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej,
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów Administratora lub strony trzeciej z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.

Jeżeli, w ocenie Administratora danych, nie zachodzi żadna z przesłanek wymienionych w art. 21 ust. 1 pozwalających na wniesienie żądania, to informuje on wnioskodawcę o niespełnieniu żądania i powodach takiej decyzji.

4. Czy dane są przetwarzane na potrzeby marketingu bezpośredniego (art. 21 ust. 2)

Jeżeli Administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, w tym profilowania, to osoba, której dane są przetwarzane ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzaniu danych w tym celu. Po wniesieniu sprzeciwu administrator nie może już przetwarzać danych w tym celu, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

5. Informacja o spełnieniu żądania

Jeżeli żądanie jest uprawnione, to Administrator danych je spełnia. Uwzględnienie sprzeciwu oznacza, że Administratorowi nie wolno już przetwarzać danych w celu objętym sprzeciwem. Nie oznacza to braku możliwości przetwarzania danych w innych celach, o ile Administrator może wskazać inną podstawę prawną przetwarzania.

Po spełnieniu żądania Administrator informuje wnioskodawcę o sposobie realizacji żądania. Informacja powinna być przekazana niezwłocznie, nie później niż w terminie 30 dni od otrzymania żądania. Termin realizacji żądania, w razie potrzeby można przedłużyć o kolejne dwa miesiące, w przypadku kiedy jego realizacja ma skomplikowany charakter. Informację o przedłużeniu terminu realizacji żądania Administrator danych przekazuje wnioskodawcy w terminie 30 dni od złożenia wniosku. Jeżeli wniosek był przekazany w formie elektronicznej, to odpowiedź powinna być również przekazana w takiej formie, chyba że wnioskodawca wskazał inną formę komunikacji.

Zał. nr 4 do Polityki

PROCEDURA ANALIZY RYZYKA

Celem procedury jest opisanie zasad przeprowadzenia analizy ryzyka, która w efekcie ma doprowadzić do zastosowania odpowiednich dla Administratora środków technicznych i organizacyjnych zapewniających obniżenie ryzyka przypadkowego lub niezgodnego z prawem zniszczenia, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Artykuł 24 RODO opisuje jeden z obowiązków Administratora Danych i brzmi następująco;

„Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane."

Każdy Administrator Danych ma więc obowiązek przeprowadzenia analizy ryzyka, żeby ustalić jego poziom w stosunku do różnych aktywów uczestniczących w przetwarzaniu. Podstawowym aktywem, którym zajmuje się RODO są dane osobowe, które należą do kategorii informacji.

W kontekście bezpieczeństwa informacji bierze się pod uwagę następujące atrybuty:

- integralność – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

- poufność – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

- dostępność – właściwość zapewniająca, że dane są dostępne zgodnie z wymaganiami użytkownika.

Wartość ryzyka (R) wylicza się według poniższego wzoru dla każdego z atrybutów bezpieczeństwa.

R = P * S

gdzie : P – prawdopodobieństwo wystąpienia zagrożenia

S – Szkodliwość skutków zmaterializowania się zagrożenia (wartość aktywa)

Sumaryczne ryzyko zmaterializowania się zagrożenia jest wyliczane według wzoru:

R = Ri + Rp +Rd

gdzie Ri – ryzyko utraty integralności

Rp – ryzyko utraty poufności

Rd – ryzyko utraty dostępności

Analizę ryzyka przeprowadza się w następujących krokach:

1. Identyfikacja aktywów biorących udział w przetwarzaniu, w tym danych osobowych i oszacowanie skutków zmaterializowania się zagrożenia.
   Przykładowe aktywa to zbiory danych osobowych, informacje uwierzytelniające, sprzęt komputerowy, usługi, w tym outsourcing, budynek. Aktywa można odpowiednio pogrupować.

Każde aktywo lub grupę aktywów należy wycenić przez pryzmat skutku zmaterializowania się zagrożenia. W jakościowej metodzie analizy ryzyka przyjmuje się, że wartość aktywa (S) jest wyrażone liczbą z przedziału 1-3, gdzie:
1 – zdarzenie wywołuje niewielki skutek (np. czas niedostępności informacji jest stosunkowo krótki, cena odtworzenia aktywa w przypadku utraty nie jest wysoka, utrata poufności dotyczy niewielkiej ilości danych),
2 – zdarzenie wywołuje znaczący skutek (np. czas niedostępności informacji lub usług systemu jest odczuwalny, cena odtworzenia aktywa jest dość wysoka, utrata poufności dotyczy szczególnych kategorii danych),
3 – zdarzenie wywołuje bardzo znaczący skutek (np. czas niedostępności jest długi i przywrócenie dostępu wiąże się z dodatkowymi kosztami, odtworzenie aktywa jest niemożliwe, utrata poufności wiąże się z koniecznością zawiadomienia Urzędu ochrony danych lub opublikowania informacji w prasie).

2. Identyfikacja zagrożeń, określanych jako potencjalne naruszenie zabezpieczenia systemu informatycznego, które będą uwzględniane w procesie analizy ryzyka.
   Źródłem zagrożeń mogą być:
   - siły wyższe np. klęski żywiołowe,
   - działania przestępcze, w tym:
     - zagrożenia związane z kradzieżą sprzętu, oprogramowania, dokumentów,
     - nieuprawnione działanie personelu,
     - nieuprawnione działanie osób postronnych,
   - błędy personelu obsługującego dokumenty tradycyjne lub system komputerowy,
   - zła organizacja pracy w tym błędy w ochronie fizycznej i technicznej,
   - awarie i uszkodzenia sprzętu i infrastruktury teleinformatycznej.

3. Szacowanie ryzyka zmaterializowania się zagrożeń dla zidentyfikowanych aktywów w kontekście wymienionych wyżej atrybutów bezpieczeństwa z zastosowaniem wzoru
   R = P * S
   gdzie prawdopodobieństwo zmaterializowania się zagrożenia przyjmuje wartości:
   1 – niskie
   2 – średnie
   3 - wysokie

   Poziom ryzyka dla poszczególnych aktywów może przyjmować wartości z przedziału 1-27.

4. Wyznaczenie poziomu ryzyka, które akceptujemy.

5. Dla wszystkich zagrożeń w stosunku do których poziom ryzyka jest wyższy - określenie i wdrożenie odpowiedniego postępowania z ryzykiem. Przez postępowanie z ryzykiem rozumie się:
   - przeniesienie ryzyka na stronę trzecią np. outsourcing usług,
   - unikanie ryzyka np. eliminacja procesów lub działań powodujących ryzyko np. zakaz wynoszenia laptopów poza teren firmy,
   - redukcję – zastosowane zabezpieczeń technicznych i organizacyjnych w celu obniżenia ryzyka np. zaszyfrowanie dysków laptopów.

   Na podstawie podjętych decyzji powstaje **Plan postępowania z ryzykiem**, który zawiera:
   - wybrane warianty postępowania z ryzykiem,

- lista zabezpieczeń do wdrożenia,
- terminy realizacji,
- osoby odpowiedzialne za wdrożenie,
- ewentualne koszty.

Ponowna analiza ryzyka powinna być przeprowadzana cyklicznie, w wyznaczonych odstępach czasu lub po znaczących zmianach w procesie przetwarzania danych osobowych.

Zał. nr 5 do Polityki

PROCEDURA OBSŁUGI NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Procedura opisuje sposób zbierania informacji o incydentach oraz realizację zadań wynikających z art. 33 i 34 RODO.

Informacje o incydentach i zdarzeniach, które mogą mieć wpływ na bezpieczeństwo danych osobowych mogą wpływać do Administratora danych i IOD, jeżeli został powołany, między innymi z następujących źródeł:
- od pracowników (obowiązek określony w Regulaminie ochrony danych osobowych),
- od ASI (Informatyka),
- z urządzeń monitorujących,
- od podmiotu przetwarzającego.

Każdy zgłoszony incydent i zdarzenie Administrator powinien zweryfikować i stwierdzić czy jest to 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.

Naruszenie ochrony danych to incydent bezpieczeństwa pociągający za sobą skutek w postaci zniszczenia, utraty, nieuprawnionego zmodyfikowania, ujawnienia lub dostępu do danych osób nieuprawnionych. Każde naruszenie ochrony danych powinno być udokumentowane i opisane w Raporcie z naruszenia ochrony danych.

Jeżeli jest mało prawdopodobne, by stwierdzone naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych Administrator danych nie ma obowiązku zgłaszać naruszenia organowi nadzorczemu.

W przeciwnym wypadku Administrator danych ma obowiązek bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić je organowi nadzorczemu. Zgłoszenie do organu nadzorczego powinno zawierać informacje opisane w art. 33 ust. 3 RODO. Zgłoszenie do organu nadzorczego powinno powstać w oparciu o Raport z naruszenia ochrony danych. Jeżeli Administratorowi nie uda się dochować 72-godzinnego terminu zgłoszenia o wystąpieniu naruszenia ochrony danych, to musi wyjaśnić przyczyny opóźnienia. Możliwa jest również sytuacja, gdy Administrator przekaże do organu nadzorczego niepełne zgłoszenie, a następnie będzie je sukcesywnie uzupełniał.

Art. 34 RODO nakłada, w niektórych przypadkach, na Administratora obowiązek zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych. Taki obowiązek powstaje, jeżeli naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Artykuł 23 ust. 1 RODO przewiduje możliwość wyłączenia w przepisach szczególnych obowiązku informowania osób o naruszeniu ochrony danych. Administrator powinien zatem sprawdzić, czy nie jest wyłączony z takiego obowiązku na mocy obowiązujących go ustaw szczegółowych.

Zawiadomienie osób, których dane dotyczą o naruszeniu ochrony danych nie jest również wymagane, gdy:

- Administrator wdrożył odpowiednie techniczne o organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności szyfrowanie, które uniemożliwia odczyt danych przez osoby nieuprawnione,
- Administrator, po stwierdzeniu naruszenia, zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą,
- powiadomienie wszystkich osób wymagałoby niewspółmiernego wysiłku – wtedy należy wydać publiczny komunikat o zdarzeniu.

Zawiadomienie osoby, której dane dotyczą o naruszeniu powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje:
- imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opis możliwych konsekwencji naruszenia ochrony danych osobowych,
- opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownym przypadku środków służących zminimalizowaniu ewentualnych negatywnych skutków naruszenia.

Zał. nr 6 do Polityki

Poniższa ankieta dotyczy oceny bezpieczeństwa przetwarzania danych osobowych przez podmiot przetwarzający (lub mający przetwarzać po zawarciu odpowiedniej umowy) dane osobowe, powierzane przez Szkołę Podstawową nr 10 im. Stefana Żeromskiego w Koszalinie
Ankieta zawiera pytania, odnoszące się do zabezpieczenia danych osobowych o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (EU) 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 ogólnym (zwanym dalej RODO).

Lp.	Pytanie	Odpowiedź
1	Czy personel podmiotu przetwarzającego został przeszkolony z zasad przetwarzania danych osobowych, zawartych w RODO?	
2	Czy podmiot przetwarzający wyznaczył osobę, mającą w swoim zakresie obowiązków dbałość o bezpieczeństwo przetwarzania danych osobowych i zarządzanie tym bezpieczeństwem?	
3	Czy do przetwarzania danych są dopuszczane wyłącznie osoby posiadające imienne upoważnienia nadane przez uprawnioną do tego osobę?	
4	Czy osoby, które zostały upoważnione do przetwarzania danych osobowych, zostały równocześnie zobowiązane do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczenia?	
5	Czy firma opracowała i wdrożyła politykę bezpieczeństwa przetwarzania danych osobowych?	
6	Czy firma posiada wdrożone procedury, umożliwiające bezzwłoczne zgłoszenie Administratorowi naruszenie bezpieczeństwa danych osobowych?	
7	Czy firma stosuje fizyczne zabezpieczenia pomieszczeń w których przetwarzane są dane osobowe przed dostępem osób nieuprawnionych? Jeśli tak, proszę opisać, jakie (np. pomieszczenia zabezpieczone drzwiami zamykanymi na klucz, została wdrożona gospodarka kluczami do pomieszczeń, system kontroli dostępu, systemy antywłamaniowe itp.).	
8	Czy jest stosowane oprogramowanie antywirusowe?	
9	Czy są stosowane środki służące ochronie danych przed ich utratą? Jakie?	
10	Czy jest zapewniona rozliczalność procesów przetwarzania danych osobowych, np. czy istnieje możliwość stwierdzenia kto i kiedy modyfikował dane konkretnej osoby?	
11	Czy umowy lub procedury serwisowe uwzględniają konieczność zapobiegania ujawnieniu chronionych danych osobom niepowołanym, np. w razie konieczności naprawy lub wymiany uszkodzonego sprzętu?	

12	Czy w przypadku przekazywania danych, podlegających ochronie, środkami telekomunikacyjnymi lub na nośnikach wymiennych, ich poufność, integralność i autentyczność jest zabezpieczana metodami kryptograficznymi (np. szyfrowanie)?	
13	Czy są stosowane środki służące ochronie danych przed nieuprawnionym dostępem? Jeśli tak, proszę je zwięźle wymienić: np. identyfikatory i hasła, systemy kontroli dostępu, firewall, itp.	
14	Czy dostęp do systemów operacyjnych komputerów, w których przetwarzane są dane podlegające ochronie, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz znanego wyłącznie uprawnionemu użytkownikowi hasła? Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?	
15	Czy każda z osób upoważnionych do przetwarzania danych loguje się do systemów, w których przetwarzane są dane osobowe własnym identyfikatorem i hasłem?	
16	Czy zastosowano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych podlegających ochronie?	

Zał. nr 7 do Polityki

Umowa powierzenia przetwarzania danych osobowych (wzór)

zawarta dnia ……. r. pomiędzy:

(zwana dalej „Umową")

……., zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**

a

……., zwaną w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

dalej występujące łącznie jako **„Strony".**

Mając na uwadze, że Strony zawarły umowę …… , w związku z wykonywaniem której Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych Strony postanowiły zawrzeć umowę następującej treści:

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1), zwanego w dalszej części „Rozporządzeniem", dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy następujące rodzaje danych osobowych: ……..

2. Powierzone przez Administratora dane osobowe będą przetwarzane przez podmiot przetwarzający wyłącznie w celu realizacji umowy …… w zakresie ……..

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim pracownikom, którzy będą przetwarzali powierzone dane.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez pracowników, których upoważnia do przetwarzania powierzonych danych, zarówno w trakcie zatrudnienia ich w podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 72 h.

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.

4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §5 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Urząd Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od …… r. na czas obowiązywania Umowy…….

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem 1 miesięcznego okresu wypowiedzenia.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§9

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora.

_____ _____

Administrator danych Podmiot przetwarzający

Zał. nr 8 do Polityki

Regulamin ochrony danych osobowych obowiązujący w Szkole Podstawowej nr 10 im. Stefana Żeromskiego w Koszalinie

1. Każda osoba dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w zakresie i celu określonym w upoważnieniu do ich przetwarzania,
    b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem obowiązków służbowych,
    c. ochrony danych osobowych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub przetwarzaniem.
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
4. Zabrania się wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia.
5. Pracownicy są zobowiązani do zabezpieczania dokumentów oraz nośników przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy np. przez zamykanie w szafach, biurkach, pomieszczeniach.
6. Zabrania się zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe zarówno
   w godzinach pracy jak i po jej zakończeniu.
7. Pracownicy zobowiązani są do stosowania zasady czystego biurka i czystego ekranu.

<u>Zasady pracy w systemach informatycznych</u>

1. Każdy pracownik zobowiązany jest do posługiwania się własnym loginem (identyfikatorem) i hasłem w celu uzyskania dostępu do systemu informatycznego.
2. Zabrania się ujawniania loginu i hasła współpracownikom i osobom z zewnątrz.
3. Zabrania się pracy w systemach informatycznych z wykorzystaniem cudzego loginu.
4. Zabrania się pracy wielu pracowników na wspólnym identyfikatorze (z wyjątkiem dostępu do komputerów wykorzystywanych przez grupę pracowników).
5. Zabrania się uruchamiania jakichkolwiek programów na prośbę innej osoby, o ile nie została ona zweryfikowana jako uprawniona. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
6. Każdy pracownik zobowiązany jest do stosowania polityki haseł obowiązującej u Administratora, która wymaga między innymi, by:
    a. hasło zawierało co najmniej 8 znaków, w tym przynajmniej jedną małą i dużą literę, cyfrę i znak specjalny,
    b. hasło było zmieniane nie rzadziej niż co 30 dni nawet gdy system tego nie wymaga,
    c. stosowane hasła były trudne do odgadnięcia,
    d. haseł nie ujawniać innym osobom,
    e. hasła przechowywać w miejscach niedostępnych dla innych osób.
7. Zabrania się wyłączania lub zmiany konfiguracji systemu antywirusowego zainstalowanego na komputerze.

8. Zabrania się przechowywania plików, które zawierają dane osobowe, na komputerach wykorzystywanych przez grupę pracowników.

Zasady korzystania z poczty elektronicznej

1. Dane osobowe przesyłane za pomocą poczty elektronicznej powinny być odpowiednio zabezpieczone (zaszyfrowane lub zabezpieczone hasłem), a hasło nie powinno być wysłane w tym samym mailu.
2. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW".
3. Użytkownicy powinni okresowo kasować maile. Dotyczy to zwłaszcza maili zawierających dane osobowe.
4. Mail służbowy jest przeznaczony do wykonywania obowiązków służbowych.
5. Zabrania się otwierania załączników (.xlsm, .exe) w mailach od nieznanych nadawców. Są to zwykle „wirusy", które mogą zainfekować komputer.
6. Zabrania się „klikać" na hiperlinki w mailach od nieznanych nadawców, gdyż mogą to być hiperlinki do stron z „wirusami".
7. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.

Zasady korzystania z internetu

1. Pracownik może korzystać z internetu wyłącznie w celach służbowych.
2. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.
3. Zabrania się włączania w opcjach przeglądarki internetowej zapamiętywania haseł.

Obowiązek zgłaszania podatności i incydentów zagrażających bezpieczeństwu danych osobowych

1. Każdy pracownik zobowiązany jest do powiadomienia zwierzchnika i jeżeli jest powołany IOD o podatnościach i incydentach, które mogą zagrażać bezpieczeństwu danych osobowych.
2. Do podatności, które wymagają powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych.
3. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (pożar, zalanie wodą),
    b. zdarzenia losowe wewnętrzne (awarie komputerów, twardych dysków, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych).
4. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    b. niewłaściwy sposób niszczenia dokumentacji,
    c. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
    d. ujawnienie osobom nieuprawnionym danych osobowych,
    e. telefoniczne próby wyłudzenia danych osobowych,
    f. kradzież, zagubienie komputerów lub nośników zawierających dane osobowe,
    g. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
    h. rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego regulaminu są naruszeniem obowiązków pracowniczych i mogą stanowić podstawę do nałożenia kary dyscyplinarnej.