Załącznik do

ZARZĄDZENIA NR 32.2018

Wójta Gminy Przytyk

z dnia 25 maja 2018 r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych

Polityka Ochrony Danych Osobowych

w

Urzędzie Gminy w Przytyku

Spis treści:

I.Postanowienia ogólne

1. Niniejszy dokument zatytułowany „Polityka Ochrony Danych Osobowych" (zwana dalej Polityką) 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 (ogólne rozporządzenie o ochronie danych -Dz. Urz. UE L 119, s. 1)

2. Celem Polityki jest ochrona podstawowych prawa i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych.

3. Niniejsza Polityka ustanawia zasady i reguły postępowania, które należy stosować oraz wskazuje działania, jakie należy wykonać, aby właściwie wykonywać obowiązki administratora danych osobowych w zakresie bezpiecznego przetwarzania danych osobowych.

II.Definicje

Używane w niniejszej Polityce definicje należy rozumieć jako;

1. **Polityka** - niniejszą Politykę Ochrony Danych Osobowych.

2. **RCPD lub Rejestr** - Rejestr Czynności(procesów) Przetwarzania Danych Osobowych.

2. **RODO** - 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).

3. **Dane** - w rozumieniu RODO 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. **Dane szczególnej kategorii** - 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.

5. **Dane karne** - dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

6. **Dane dzieci** - dane osób poniżej 16. roku życia.

7. **Osoba** - osobę, której dane osobowe dotyczą.

8. **Przetwarzanie danych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie,

utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

8. Naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

10. Zgoda - zgoda osoby, której dane dotyczą oznacza dobrowolne i świadome, konkretne i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

11. Administrator danych - osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; (Gmina Przytyk);

12. IOD lub Inspektor - Inspektora Ochrony Danych Osobowych;

13. Podmiot przetwarzający - organizację lub osobę, której powierzono przetwarzanie danych osobowych.

14. Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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 nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

15. Organ nadzorczy - niezależny organ publiczny ustanowiony przez państwo zgodnie z art. 51 RODO

III. Deklaracja intencji, zasady ochrony danych

1. Administrator danych zapewnia bezpieczeństwo przetwarzania danych osobowych, określa kierunki postępowania oraz wspiera inicjatywy związane z ochroną danych.
2. Administrator danych deklaruje przetwarzane danych osobowych z poszanowaniem następujących zasad:
a) legalności – przetwarzania danych wynikających określonych przepisów prawa,
b) rzetelności i prawidłowości – z dołożeniem należytej staranności,
c) przejrzystości – czytelnej dla osoby, której dane dotyczą,
d) minimalizacji – adekwatności w stosunku do celu,
e) bezpieczeństwa danych i czasowości - bezpiecznie i nie dłużej niż potrzeba.
3. Istota ochrony danych opiera się na następujących filarach:
a) legalności to jest dbałości o ochronę prywatności i przetwarzania danych zgodnie z prawem,
b) bezpieczeństwie utrzymującym się stale na odpowiednim poziomie,
c) poszanowaniu praw jednostki umożliwiającym wykonywanie praw osobom, których dane są przetwarzane,

d) rozliczalności polegającej na dokumentowaniu spełniania przez Administratora danych swoich obowiązków w sposób umożliwiający wykazanie w każdej chwili zgodności przetwarzania z wymogami ochrony prywatności osób, których dane są przetwarzane.

4. Wszyscy, którzy przetwarzają dane osobowe mają obowiązek zapoznać się z zasadami ochrony danych osobowych opisanymi w niniejszym dokumencie oraz stosować je w wykonywaniu przypisanych zadań.

5. Polityka zawiera zasady ochrony danych wyjaśniające przyjęte standardy i wymagania, a także załączniki uszczegóławiające zakresy ochrony danych (rejestry, instrukcje).

IV.Kompetencje i odpowiedzialność Administratora danych oraz Inspektora. Obowiązki związane z przetwarzaniem danych.

1. Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Administrator danych, zapewniające prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnianie osobom nieuprawnionym, przetwarzaniem z naruszeniem RODO oraz utratą, uszkodzeniem lub zniszczeniem, a do jego do kompetencji należy w szczególności:

a) określenie celów i zasad ochrony danych osobowych,

b) wyznaczanie IOD,

c) przyjmowanie i zatwierdzanie niezbędnych dokumentów, wymaganych przez RODO regulujących ochronę danych osobowych u Administratora danych, a także zapewnienie realizacji pozostałych obowiązków wskazanych w RODO.

2. Odpowiedzialnym za nadzór i monitorowanie przestrzegania Polityki jest Inspektor, który zgodnie z art. 37 ust. 1 RODO w ramach swoich zadań dba o zapewnienie zgodności przetwarzania z przepisami dotyczącymi ochrony danych osobowych, a w szczególności:

a) zachowuje w tajemnicy lub poufności szczegóły wykonywanych zadań,

b) informuje Administratora danych, Podmiot przetwarzający oraz osoby, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich w związku z ochroną danych osobowych,

c) prowadzi działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

d) współpracuje z organem nadzorczym i pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych (w tym z uprzednimi konsultacjami zgodnie z art. 36).

e) udziela informacji osobom, których dane dotyczą informacji zgodnie z przysługującymi im prawami.

3. Odpowiedzialną za zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych jest wyznaczona przez Administratora danych osoba, która w szczególności zapewnia:

a) przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa,

b) udział w przeprowadzanych przez Inspektora kontrolach ochrony przetwarzanych danych osobowych,

c) kontrolę przepływu informacji pomiędzy systemem informatycznym, a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,

d) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną,

e) utrzymanie systemów informatycznych w należytej sprawności technicznej,

f) bieżącą współpracę z Inspektorem .

4. Odpowiedzialnymi za stosowanie niniejszej Polityki są wszystkie osoby, które mają dostęp do przetwarzania danych osobowych bez względu na zajmowane stanowisko oraz miejsce aktywności zawodowej, stosunek pracy jak również osoby fizyczne świadczące usługi na rzecz Administratora danych w ramach umów cywilnoprawnych oraz inne osoby (praktykanci, stażyści)

5. Niezależnie od niniejszych zasad opisanych w Polityce w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

V. System ochrony danych osobowych

Na system ochrony danych składają się następujące elementy:

1. Rejestr Czynności Danych Osobowych jako podstawowe narzędzie rozliczania zgodności z ochroną danych.

2. Inwentaryzacja danych i ich weryfikacja - polegające na identyfikacji zasobów danych osobowych (dane zwykłe i dane szczególnej kategorii, dane dzieci i ich wykorzystania) oraz weryfikacji podstawy prawnej (jednostka identyfikuje i opisuje w rejestrze podstawy prawne przetwarzania danych osobowych).

3. Minimalizacja - stosowane są zasady i metody zarządzania minimalizacja (privacy by default) poprzez stosowanie zasady adekwatności danych do celu ich przetwarzania, ograniczonego dostępu do danych i zarządzania okresem ich przechowywania.

4. Zarządzanie prawami osoby – Administrator danych stosuje procedury pozwalające na spełnianie obowiązku informacyjnego wobec osób, których dane przetwarza i wypełnia prawa tych osób poprzez realizację obowiązków informacyjnych, weryfikację i możliwość wypełnienia żądań, zawiadamianie o naruszeniach w uzasadnionych przypadkach.

5. Bezpieczeństwo – zapewniany i zachowywany jest odpowiedni poziom bezpieczeństwa danych poprzez:

a) przeprowadzanie nieformalnej lub formalnej analizy ryzyka dla czynności (procesów) przetwarzania danych,

b) przeprowadzenia oceny skutków dla ochrony danych, tak gdzie ryzyko naruszenia praw jest wysokie,

c) dostosowywanie środków ochrony do ustalonego ryzyka,

d) wykorzystanie elementów zarządzania bezpieczeństwem informacji,

e) zarządzanie incydentami poprzez stosowanie procedur identyfikujących naruszenie ochrony danych osobowych, oceniających skutki naruszenia, w uzasadnionym przypadku zgłaszania do instytucji nadzoru,

f) sposób zachowania i postępowania w sytuacjach krytycznych.

6. Środki organizacyjne i techniczne zastosowane do zapewnienia poufności, integralności i dostępności przetwarzania

7. Zabezpieczenie dokumentacji papierowej i elektronicznej przed utratą, zniszczeniem, ujawnieniem i dostępem osób nieupoważnionych, niszczenie dokumentacji i likwidacja sprzętu komputerowego

VI. Rejestr czynności (procesów) przetwarzania

1. Rejestr czynności (procesów) przetwarzania danych stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady rozliczalności, na której opiera się cały opisywany w RODO system ochrony danych osobowych.

2. W prowadzonym Rejestrze inwentaryzuje się i monitoruje sposób wykorzystania danych osobowych w związku z realizacją ustawowych zadań podmiotu przetwarzającego dane.

3. Rejestr jest jednym z podstawowych narzędzi umożliwiających rozliczenie się z większości obowiązków ochrony danych osobowych odnotowywanych w rejestrze:

a) cel przetwarzania,

b) kategorie osób i kategorie danych,

c) podstawa prawna przetwarzania,

d) źródło danych – sposób pozyskania,

e) kategorie odbiorców ,

f) podmiot przetwarzający,

g) ogólny opis organizacyjnych i technicznych środków ochrony danych,

h) inne dane (w razie konieczności) i aktualizacje.

4. Rejestr obejmuje wszystkie procesy przetwarzania danych osobowych, które zachodzą u Administratora danych oraz u Przetwarzającego według wzoru Rejestru stanowiącego załącznik nr 1 do niniejszej Polityki.

VII. Inwentaryzacja danych i weryfikacja podstawy ich przetwarzania

1. W ramach inwentaryzacji identyfikowane są następujące dane:

a) szczególnej kategorii i dane karne dla zapewnienia ich przetwarzania zgodnie z zasadami ich ochrony,

b) dane niezidentyfikowane, które mogą być przetwarzane dla realizacji praw osób, których dotyczą,

c) dane dla których Administrator danych jest lub może być współadministratorem.

2. W ramach identyfikacji i rejestracji podstaw prawnych spełnione powinny być następujące warunki:

a) w razie potrzeby - obok wskazania w dokumentach ogólnej podstawy prawnej (zgoda, umowa, obowiązek prawny, zadanie publiczne, żywotny interes) - konieczność dookreślenia podstawy w precyzyjny i czytelny sposób

b) zarządzanie zgodami polegające na rejestracji i weryfikacji zgody dla konkretnego celu, jej cofnięcia lub odmowy,

c) osoby przetwarzające dane osobowe, w szczególności kierownicy komórek organizacyjnych mają obowiązek znajomości podstawy prawnej, na podstawie której dokonują konkretnych czynności (procesów) przetwarzania.

VIII. Minimalizacja przetwarzania danych

Administrator danych stosuje zasadę minimalizacji przetwarzania danych osobowych w odniesieniu do adekwatności (ilości danych niezbędnych dla zrealizowania celu), dostępu do nich i czasu ich przydatności poprzez:

1. Minimalizację zakresu (adekwatność), polegającą na tym , że Administrator danych :

a) zweryfikował zakres pozyskiwanych danych, zakres przetwarzanych danych i ilość przetwarzanych danych pod katem adekwatności do celów przetwarzania w ramach wdrożenia RODO,

b) dokonuje okresowo, nie rzadziej niż raz na rok przeglądu przetwarzanych danych i przeprowadza weryfikację zasady minimalizacji danych w ramach procedur zarządzania zmianą (privacy by design).

2. Minimalizację dostępu polegającą na tym, że Administrator danych:

a) stosuje ograniczenia dostępu do danych osobowych – środki ochrony - organizacyjne, techniczne , fizyczne,

b) dokonuje okresowego przeglądu dostępu do danych (przegląd użytkowników systemu, kontrola dostępu fizycznego) nie rzadziej niż raz na rok,

c) stosuje szczegółowe zasady kontroli dostępu logicznego i fizycznego zawarte są w procedurach bezpieczeństwa informacji i bezpieczeństwa fizycznego.

3. Minimalizację czasu polegającą na tym, że Administrator danych:

a) wdraża kontrolę weryfikacji dalszej przydatności danych osobowych w stosunku do terminów wskazanych w Rejestrze.

b) dane nieprzydatne wraz z upływem czasu usuwane są z akt albo archiwizowane zgodnie z zasadami archiwizacji.

IX. Zarządzanie prawami osoby, obowiązki informacyjne i żądania osób

1. Jednostka dba o czytelność informacji i komunikacji z osobami, których dane przetwarza oraz dotrzymywanie w miarę możliwości realnych terminów realizacji obowiązków względem tych osób.

2. Prowadzane są adekwatne metody identyfikacji i uwierzytelnienia osób oraz procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób, wprowadzać zmiany, integrować, usuwać dla potrzeb realizacji praw jednostki.

3. Ułatwia się osobom korzystanie z ich praw poprzez publiczną informację na stronie internetowej informacji lub od wołań (linków) do informacji o prawach osób. Określa się także sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie jest to możliwe (tablica informacyjna o monitoringu wizyjnym)

4. Określa się efektywne i zgodne z prawem sposoby wykonywania obowiązków informacyjnych wobec osób, których dane są przetwarzane połączone z dokumentowaniem wypełnienia obowiązków informacyjnych, w tym zawiadomienia i żądania osób.

5. Jednostka informuje osobę o przetwarzaniu jej danych przy pozyskiwaniu danych od tej osoby.

6. Przy przetwarzaniu danych osoby pozyskanych niebezpośrednio od niej jednostka informuje ta osobę.

7. Najpóźniej przy pierwszym kontakcie z osoba jednostka informuje ją o prawie sprzeciwu względem przetwarzania jej danych osobowych.

8. Jednostka informuje osobę o zmianie celu przetwarzania, o uchyleniu ograniczenia przetwarzania (przed uchyleniem)

9. Jednostka informuje odbiorców danych(jeżeli to będzie możliwe lub nie będzie wymagało niewspółmiernie dużego wysiłku) o sprostowaniu, ograniczeniu przetwarzania lub usunięciu danych.

10. Jednostka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych w przypadku uzasadnionego wysokiego ryzyka naruszenia praw lub wolności tej osoby.

11. W wypadku żądania osoby dotyczącego informacji na temat przetwarzania jej danych osobowych:

a) jeżeli nie przetwarza się danych osoby żądającej informacji o przetwarzaniu jej danych, informuje się tym zainteresowaną osobę,

b) jeżeli jest to uzasadnione Administrator danych informuje osobę w okresie miesiąca od otrzymania żądania o odmowie rozpatrzenia żądania ujawnienia, czy jej dane są przetwarzane poucza o prawach osoby z tym związanych (jeżeli rozpatrywanie żądania trwa dłużej niż miesiąc należy o tym poinformować zainteresowana osobę),

c) realizując prawa osób, których dane dotyczą Administrator danych uwzględnia także prawa i wolności osób trzecich.

d) Administrator danych może zwracać się do osoby żądającej udostępnienia danych dla wyjaśnienia wątpliwości, co naruszenia wolności osoby trzeciej, może odmówić zadośćuczynienia żądaniu.

12. Dostęp osoby do danych, kopie danych może mieć miejsce w następujących przypadkach

a) Administrator danych informuje osobę o przetwarzaniu i zakresie tego przetwarzania (odpowiadającym obowiązkowi informacyjnemu przy zbieraniu danych) zgodnie z art. 15 RODO oraz udziela osobie dostępu do danych jej dotyczących,

b) dostęp do danych może zostać zrealizowany przez wydanie kopii danych, z odnotowaniem faktu jej wydania. Pierwsza kopia jest bezpłatna, następne są płatne skalkulowane na podstawie oszacowanego jednostkowego kosztu.

13. Przenoszenie danych następuje na żądanie osoby, wtedy Administrator danych wydaje tej osobie lub za jej zgodą innemu podmiotowi dane tej osoby w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane w celu realizacji umowy.

14. Sprostowanie, uzupełnienie danych może nastąpić, gdy

a) Administrator danych dokonuje sprostowania danych jej dotyczących, a na żądanie osoby informuję ją o odbiorcach danych, może odmówić sprostowania w sytuacji niewykazania przez żądającą osobę nieprawidłowości danych,

b) Administrator danych uzupełnia i aktualizuje dane na żądanie osoby, może też odmówić w wypadku niezgodności z celem przetwarzania danych.

15. Ograniczenie przetwarzania następuje na żądanie osoby, kiedy

a) osoba kwestionuje prawidłowość danych, wtedy ogranicza się przetwarzanie do czasu wyjaśnienia,

b) przetwarzanie jest niezgodne z prawem,

c) dane osobowe nie są Administratorowi danych potrzebne, a są potrzebne osobie, której dotyczą i wiążą się z jej roszczeniami,

d) osoba wniosła sprzeciw względem przetwarzania związany z jej szczególną sytuacją, ograniczenie trwa do czasu stwierdzenia że istnieją uzasadnione podstawy przetwarzania - związane z realizowanym zadaniem publicznym - nadrzędne wobec podstaw sprzeciwu. (jeżeli nie zachodzą takie podstawy jednostka uwzględnia sprzeciw).

16. Sprzeciw nie jest uwzględniany przy badaniach naukowych, historycznych, przetwarzaniu dla celów statystycznych realizowanych do wykonania zadania realizowanego w interesie publicznym (innym wypadku wniesiony umotywowany szczególna sytuacja sprzeciw jest skuteczny).

17. Usunięcie danych następuje na żądanie osoby, gdy:

a) dane nie są konieczne dla celów, dla których zostały zebrane,

b) została cofnięta zgoda , a innej podstawy przetwarzania nie ma,

c) osoba wniosła skuteczny sprzeciw względem przetwarzania danych,

d) dane były przetwarzane niezgodnie z prawem albo usuniecie wynika z obowiązku prawnego,

e) żądanie dotyczy danych dziecka zebranych na podstawie zgody (dane na stronie internetowej dotyczące udziału w konkursie),

f) jeżeli dane podlegające usunięciu zostały upublicznione jednostka podejmuje rozsądną akcję informacyjną w stosunku do innych podmiotów(administratorów) przetwarzających te dane o potrzebie usunięcia tych danych i zaprzestaniu ich udostępniania.

18. Ramowa klauzula informacyjna o przetwarzaniu danych osobowych stanowi załącznik nr 2 do niniejszej Polityki

X. Bezpieczeństwo danych osobowych

Jednostka w związku z przetwarzaniem danych osobowych zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych poprzez następujące procesy:

1. Analizę ryzyka i adekwatności środków bezpieczeństwa oraz ocenę skutków:

a) przeprowadza i dokumentuje analizę ryzyka przy zapewnieniu odpowiedniej wiedzy o bezpieczeństwie informacji i ciągłości działania, grupując dane i procesy pod kątem ryzyka,

b) przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności (procesów) przetwarzania o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, uwzględniając charakter, zakres, kontekst i cele przetwarzania,

c) stosuje środki organizacyjne i techniczne środki bezpieczeństwa zapewniające zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

d) prowadzi monitorowanie zabezpieczeń systemów teleinformatycznych i okresowe kontrole przestrzegania zapisów Polityki przez pracowników w zakresie bezpiecznego użytkowania tych systemów,

e) stosuje środki dla zapewnienia ciągłości działania, uwzględnia się w szczególności ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych aby zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

f) zarządza incydentami i stosuje Instrukcje postępowania w sytuacjach kryzysowych stanowiącą załącznik nr 3 do niniejszej Polityki,

g) dokonuje oceny skutków planowanych operacji przetwarzania, tam gdzie zgodnie z analiza ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

2. Stosowanie organizacyjnych, technicznych i fizycznych środków bezpieczeństwa uwzględniających wyniki analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków przetwarzania dla praw i wolności osób.

3. Postępowanie w sytuacji kryzysowej i zgłaszanie naruszeń:

a) stosuje się procedury pozwalające na identyfikację, ocenę i ewentualne zgłoszenie naruszenia ochrony danych osobowych.

b) prowadzi się Rejestr naruszeń danych osobowych stanowiący załącznik nr 4 do niniejszej Polityki

5. Postępowanie w sytuacjach krytycznych należy:

a) pożar, zalanie – powiadomić straż pożarną (numer telefonu alarmowy 112) i jeśli nie jest zagrożone własne lub czyjeś zdrowie lub życie przystąpić do ratowania dokumentacji,

b) kradzież – bezzwłocznie powiadomić organy ścigania (numer telefonu alarmowy 112) i udzielić im wszelkiej pomocy w ujęciu sprawcy,

3) klęska żywiołowa – współdziałać ze służbami ratowniczymi i początkowymi przy ratowaniu dokumentacji (również innego mienia).

XI. Środki organizacyjne i techniczne zastosowane do zapewnienia poufności, integralności i dostępności przetwarzania danych

1. Dla bezpiecznego przebiegu procesów przetwarzania danych stosuje się następujące środki organizacyjne:

a) powołanie Inspektora ochrony danych wraz z przypisaniem mu zadań i jego oświadczeniem o należytym wykonywaniu powierzonej funkcji, wg wzoru stanowiącego załącznik nr 5 do niniejszej Polityki,

b) wyznaczenie osoby odpowiedzialnej za bezpieczne administrowanie systemami informatycznymi i przypisanie jej konkretnych zadań.

c) opracowanie Rejestru czynności(procesów) przetwarzania danych,

d) opracowanie i wdrożenie Polityki bezpieczeństwa przetwarzania danych osobowych

e) dopuszczenie do przetwarzania danych osób z upoważnienia i polecenia Administratora danych,

f) okresowe szkolenie z zakresu ochrony danych osobowych, a fakt uczestnictwa szkoleniu potwierdzony pisemnie na liście obecności uczestników szkolenia (każdy nowo przyjęty pracownik obowiązkowo odbywa szkolenie przed przystąpieniem do przetwarzania danych),

g) przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań i obowiązków służbowych, a zakres upoważnień wynika z zakresu tych zadań i obowiązków.

h) dane osobowe powinny być wyłącznie przetwarzane w miejscach do tego przystosowanych i zabezpieczonych, przez osoby upoważnione przez Administratora danych, a dostęp zarówno do obszarów przetwarzania danych (budynków, pomieszczeń) jak i do urządzeń przetwarzających dane osobowe powinny mieć wyłącznie osoby uprawnione; przebywanie osób nieuprawnionych w w/w obszarze jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

2. Każda osoba mająca dostęp do danych osobowych:

a) składa pisemne oświadczenie o zapoznaniu się z treścią niniejszej Polityki i RODO oraz zobowiązuje się do przestrzegania zawartych w nich przepisów,

b) po złożeniu powyższego oświadczenia Administrator danych wydaje tej osobie upoważnienie do przetwarzania danych i polecenie do przetwarzania danych osobowych w zakresie wynikającym z realizowanych zadań i wypełnianych obowiązków, wg wzoru stanowiącego załącznik nr 6 do niniejszej Polityki ,a podpisany dokument jest włączany do akt osobowych tej osoby'

3) Dane osobowe mogą zostać powierzone do przetwarzania w drodze umowy określającej zakres i cel przetwarzania przez inny podmiot stosujący odpowiednie środki organizacyjne i techniczne zgodne z wymogami RODO, wg wzoru umowy stanowiącego załącznik nr 7 do niniejszej Polityki.

4. Dla bezpiecznego przebiegu procesów przetwarzania danych stosuje się następujące środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:

a) dostęp do systemu operacyjnego w którym przetwarzane są dane osobowe komputera posiada wyłącznie osoba administrująca systemem; dostęp zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora oraz hasła,

b) zastosowano środki ochrony przed szkodliwym oprogramowaniem,

c) użyto system Firewall jako element programu antywirusowego do ochrony dostępu do sieci komputerowej,

d) dostęp do urządzeń aktywnych sieci mają wyłącznie komputery które uzyskały zgodę na prace w sieci.

5. Dla bezpiecznego przebiegu procesu przetwarzania stosuje się następujące środki ochrony w ramach systemowych narzędzi programowych i baz danych

a) dostęp do procesów przetwarzania danych osobowych wymaga uwierzytelnienia z wykorzystaniem spersonalizowanego identyfikatora użytkownika oraz unikatowego hasła użytkownika, związanego z wcześniej wydanym przez Administratora danych upoważnieniem i poleceniem przetwarzania danych,

b) zmiana haseł dostępowych następuję przynajmniej raz na 30 dni,

c) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,

d) osoba odpowiedzialna za systemy informatyczne sporządza okresowo kopie bezpieczeństwa danych osobowych ze wszystkich wykorzystywanych w systemów informatycznych, programów, żeby zabezpieczyć się przed utrata danych spowodowaną awarią sprzętu komputerowego,

e) należy zabezpieczyć komputery, serwer przed skutkami awarii bądź niestabilnego napięcia z sieci elektrycznej poprzez podłączenie każdego komputera, serwera do zasilacza UPS o odpowiedniej mocy.

6. Administrator danych za pośrednictwem IOD i osoby administrującej systemami informatycznymi lub innej upoważnionej osoby prowadzi i dokumentuje monitoring przetwarzania danych poprzez okresowe sprawdzanie:

a) przestrzegania zabezpieczeń fizycznych przez osoby przetwarzające dane,

b) działania zabezpieczeń przed zagrożeniami pochodzącymi z sieci publicznej,

c) działania oprogramowania zabezpieczającego przed uzyskaniem nieuprawnionego dostępu do systemów,

d) działania urządzeń zabezpieczających systemy teleinformatyczne przed skutkami awarii zasilania oraz sprawdzania kopii bezpieczeństwa pod względem przydatności do odtworzenia danych.

7. Nadzór nad sprzętem komputerowym wymaga uwzględnienia następujących faktów:

a) sprzęt komputerowy jest sprzętem nie wymagającym systematycznej okresowej kontroli stanu technicznego (nie stwarza zagrożenia dla użytkownika ani dla zainstalowanego w nim oprogramowania sam z siebie, jedynie na skutek działania czynników zewnętrznych, na przykład przepięcia w sieci elektrycznej), dlatego zrezygnowano z przeprowadzania systematycznych okresowych przeglądów takiego sprzętu), stan ilościowy sprzętu oraz oprogramowania jest sprawdzany w ramach inwentaryzacji,

b) nadzór nad sprzętem technicznym sprawuje Administrator danych za pośrednictwem merytorycznie przygotowanej osoby i to ona reaguje na wszelkiego typu zgłoszenia od pracowników – użytkowników systemu informatycznego dotyczące nieprawidłowego działania sprzętu czy też oprogramowania. (w wypadku większej awarii do czasu jej usunięcia wyłącza z eksploatacji sprzęt komputerowy naklejając w widocznym miejscu kartkę z informacją „Urządzenie Niesprawne" i informuje o tym użytkowników, bądź zabiera ze sobą sprzęt komputerowy w celu jego naprawy).

8. Nadzór nad zainstalowanym oprogramowaniem na komputerach będących własnością Administratora danych następuje za pośrednictwem osoby administrującej systemami informatycznymi i IOD – osoby te dokonują okresowej kontroli danych zawartych w komputerze. (jeżeli w wyniku takiej wyrywkowej kontroli wyjdzie na jaw że użytkownik dokonał samowolnej instalacji jakiegokolwiek oprogramowania na które Administrator danych nie posiada licencji, bądź nie spełnia wymogów licencyjnych, odpowiada za to bezpośrednio użytkownik komputera).

9. Użytkownik czuwa nad tym, żeby zgodnie z procedurami wewnętrznymi określonymi w Polityce nie zostawiać komputera zalogowanego i to on odpowiada za wszystkie zmiany w oprogramowaniu i sprzęcie niezgodne z zapisami w Polityce.

10.Taka sama forma odpowiedzialności obowiązuje w wypadku kontroli przez organy upoważnione do kontroli legalności oprogramowania. Za oprogramowanie zewidencjonowane w kartach komputerów i za wszystkie licencje będące własnością Administratora danych odpowiada sam administrator, a IOD nadzoruje zgodność z wymogami licencyjnymi oprogramowania użytkowanego i będącego własnością Administratora danych.

XII. Zabezpieczenie dokumentacji papierowej i elektronicznej przed utratą, zniszczeniem, zmianą, sfałszowaniem i dostępem osób nieupoważnionych, niszczenie dokumentacji i likwidacja sprzętu komputerowego

1. Dokumentacja w formie papierowej i elektronicznej zawierająca dane osobowe różnych kategorii danych powinna być szczególnie chroniona na każdym etapie swojego użytkowania i zabezpieczona przed jej utratą, zniszczeniem, zmianą, sfałszowaniem i dostępem osób nieupoważnionych.

2. Dokumentacja w formie papierowej zawierająca dane osobowe:

a) powinna być przechowywana od momentu powstawania do momentu zniszczenia w warunkach zabezpieczenia jej przed swobodnym i nieuprawnionym dostępem, wypłynięciem, ujawnieniem oraz zniszczeniem, a dokumenty po wykorzystaniu i utracie przydatności należy niszczyć w sposób mechaniczny za pomocą niszczarek dokumentów,

b) w momencie użytkowania nie można dokumentów pozostawić bez dozoru osób uprawnionych,

c) dokumentację archiwizujemy w wyodrębnionym pomieszczeniu (składnica akt/archiwum), w których powinno się systematycznie monitorować temperaturę i wilgotność; dostęp do pomieszczenia archiwum mają wyłącznie osobowy upoważnione przez Administratora danych,(po ustaniu okresu archiwizacyjnego dokonuje się zniszczenia dokumentacji, z której sporządza się protokół zniszczenia).

3. Dokumentację w formie elektronicznej zawierającą dane osobowe zabezpiecza się w następujący sposób:

a) dostęp do dokumentacji mają tylko zalogowani użytkownicy systemu informatycznego z odpowiednimi uprawnieniami i możliwością identyfikacji użytkowników odpowiadających za dane edytowane bądź wprowadzone,

b) przed zniszczeniem tych danych system zabezpieczony jest urządzeniami chroniącymi fizycznie system oraz poprzez regularne sporządzanie kopii bezpieczeństwa przechowywane są w wyznaczonym miejscu,

c) użytkownicy mają tak dobrane uprawnienia żeby ograniczyć do minimum możliwość wypływu informacji oraz ich przekłamania lub zmiany; do programu komputerowego wprowadza się dane po ich fizycznej autoryzacji przez osoby uprawnione.

d) kopie bezpieczeństwa (kopie zapasowe) przechowuje się miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją uszkodzeniem lub zniszczeniem, a dostęp do niego mają wyłącznie upoważnione osoby na podstawie wydanego upoważnienia przez Administratora danych.

4. W razie konieczności likwidacji sprzętu komputerowego, nośników danych i elementów eksploatacyjnych konieczne jest zapewnienie bezpiecznej procedury stosowanej w wypadku kasacji i utylizacji poprzez :

a) sprzęt wycofany z eksploatacji, trwale uszkodzony lub wyeksploatowany mogący zawierać dane osobowe zgłasza się niezwłocznie bezpośrednio do Administratora danych,

b) kasacje należy poprzedzić zgromadzeniem w jednym miejscu sprzętu do kasacji przez Inspektora,

c) przed zniszczeniem należy pozbawić sprzęt komputerowy oraz nośniki danych wszystkich informacji możliwych do odczytu,

d) w wypadku nośników zewnętrznych nośników danych (dyski zewnętrzne, płyty DVD, CD-R, pendrive) proces kasacji zostaje przeprowadzony przez Inspektora w obecności osoby odpowiedzialnej za administrowanie systemów informatycznych, a z przeprowadzonej kasacji sporządza się protokół zniszczenia,

e) nośniki danych należy zniszczyć w taki sposób, aby stało się niemożliwe odzyskanie z nich jakichkolwiek danych, dyski twarde uszkodzone lub wyłączone z eksploatacji przed oddaniem do utylizacji należy trwale pozbawić zapisu lub zniszczyć dysk twardy w ten sposób aby niemożliwym stało się odzyskanie informacji .

f) należy także pamiętać o obowiązku ewentualnego zgłoszenia listy sprzętu komputerowego i nośników danych do pracownika odpowiedzialnego za prowadzenie ewidencji rzeczowych składników majątku (środków trwałych, wartości niematerialnych i prawnych, pozostałych środków trwałych, wyposażenia).

XIII. Postanowienia końcowe

1. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy 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 (ogólne rozporządzenie o ochronie danych - Dz. Urz. UE L 119, s. 1).

2. Dla zapewnienia odpowiedniego stopienia bezpieczeństwa odpowiadającego ryzyku naruszenia praw i wolności osób fizycznych oraz mając na uwadze zmiany przepisów szczegółowych w zakresie ochrony danych, Administrator Danych będzie dokonywać corocznie aktualizacji treści zawartej w niniejszej Polityce i dokonywać stosownych zapisów w Rejestrze czynności (procesów) przetwarzania danych .

3. Niezależnie od wymagań wskazanych w rozporządzeniu (RODO) obowiązują dodatkowo wymagania wynikające z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity Dz. U. z 2014 r. poz. 1114.), w tym głównie wymagania wskazane w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności.

4. Zapewnienie skutecznej ochrony danych osobowych wymaga przestrzegania zasad postępowania z dokumentacją określonych w Rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie

instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. 2011 nr 14 poz. 67)

XIV. Spis załączników

1) załącznik nr 1 – Rejestr czynności (procesów) przetwarzania danych
2) załącznik nr 2 – wzór Karty (klauzuli) Informacyjnej
3) załącznik nr 3 - Instrukcja postępowania w sytuacjach naruszenia ochrony danych
4) załącznik nr 4 – Rejestr naruszeń danych
5) załącznik nr 5 –wzór powołania IOD
6) załącznik nr 6 – wzór upoważnienia do przetwarzania danych (z oświadczeniem)
7) załącznik nr 7 – wzór umowy o powierzenie przetwarzania danych