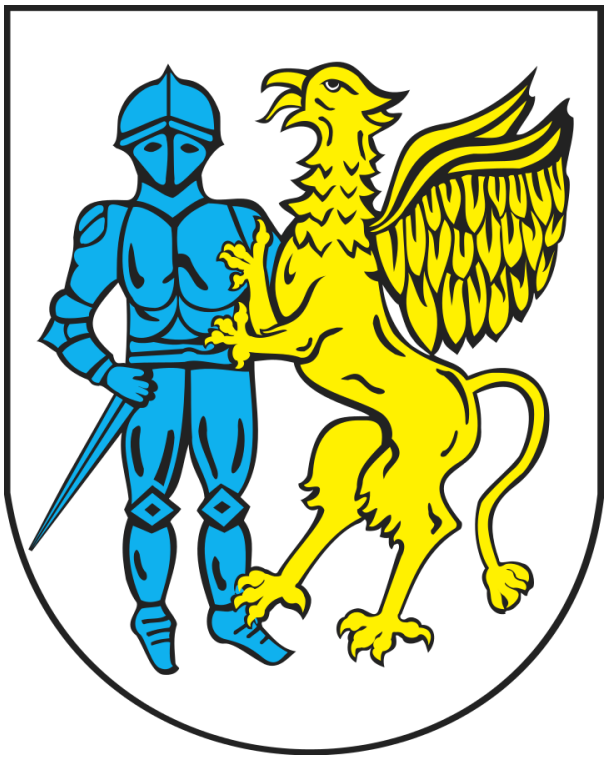
Załącznik do zarządzenia nr 96/2019r.
Burmistrza Gminy i Miasta Gryfów Śląski

POLITYKA OCHRONY DANYCH OSOBOWYCH

URZĄD GMINY I MIASTA GRYFÓW ŚLĄSKI



ROZDZIAŁ I
Postanowienia ogólne

§ 1 Wstęp

1. Polityka ochrony danych zwana dalej „Polityką”, jest dokumentem określającym środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu, a także ma za zadanie usprawnienie i usystematyzowanie organizacji pracy Administratora.
2. Polityka została opracowana zgodnie z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, zwane dalej RODO) i ma na celu wykazanie, że przetwarzanie danych odbywa się zgodnie z tym rozporządzeniem.

§ 2 Definicje

Ilekroć w Polityce jest mowa o:

1. **Administratorze Danych/Administratorze** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, w ramach niniejszego dokumentu jest to Burmistrz Gminy i Miasta Gryfów Śląski;
2. **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 s. 1);
3. **Dane osobowe** – to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego,

umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej;

4. **Zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony na funkcje;
5. **Przetwarzaniu danych** – rozumie się przez to to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych;
6. **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
7. **Kartotece** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, decyzji, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierający dane osobowe;
8. **Inspektorze Ochrony Danych Osobowych (IOD)** – to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i tej polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego;
9. **Administratorze Systemów Informatycznych (ASI) –** rozumie się przez to osobę odpowiedzialną za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację wyznaczonego przez Administratora Danych;
10. **Użytkowniku** – rozumie się osobę upoważnioną przez Administratora danych Osobowych do przetwarzania danych osobowych w systemie informatycznym oraz w kartotekach;
11. **Pomieszczeniach** – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

§ 3 Cele

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenie fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz poprzez użytkowników.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   a) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
   b) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   c) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   d) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

§ 4 Sposoby realizacji celów

Realizację zamierzeń określonych w § 3 powinny zagwarantować następujące założenia:

1. wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych oraz ich odpowiedzialność za ochronę tych danych;
2. przeszkolenie pracowników w zakresie bezpieczeństwa i ochrony danych osobowych;
3. upoważnienie użytkowników do przetwarzania danych osobowych oraz przypisanie użytkownikom określonych atrybutów umożliwiających wykonywanie ustalonych operacji na różnych poziomach zbiorów danych osobowych – stosowanie do indywidualnego zakresu upoważnienia, zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień,
4. Podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń;
5. Okresowe sprawdzenie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
6. Opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;

7. Śledzenie osiągnięć w dziedzinie zabezpieczenia systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno-finansowych – wdrożenie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5 Naruszenie ochrony danych osobowych

Za naruszenie ochrony danych osobowych uważa się w szczególności:

1. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
2. naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jak błąd w działaniu osoby uprawnionej (np. zmianę zawartości, danych, utratę całości lub części danych),
3. naruszenie lub próby naruszenia integralności systemu,
4. zmianę lub utratę danych zapisanych na kopii zapasowych,
5. naruszenie lub próby naruszenia poufności danych lub ich części,
6. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu)
7. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
8. zniszczenie, uszkodzenie lub wszelkie próby integracji nieuprawnionej w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodny z przeznaczeniem) danych zawartych w systemie informatycznym lub kartotekach,
9. inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,

Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II

Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych

§ 6 Analiza ryzyka

Procedura szacowania ryzyka, na którą składają się analiza i ocena ryzyka jest niezbędnym elementem prawidłowego zrealizowania ciążącego na Administratorze obowiązku wdrożenia odpowiednich środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Ogólna analiza ryzyka stanowi załącznik nr 1, do niniejszej polityki.

§ 7 Zapewnienie zgodności z przepisami RODO

Administrator zobowiązany jest do spełnienia obowiązków prawnych wynikających z RODO. Należy przede wszystkim zapewnić, że :

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas – zasada ograniczonego czasu,
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
5. opracowano klauzule informacyjne dla powyższych osób,
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

§ 8 Ocena skutków

Ocena skutków jest formalną, wymaganą w określnych w art. 35 RODO przypadkach procedurą, za wykonanie, której odpowiada Administrator. W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem oraz po wyrażeniu przez niego opinii.

§ 9 Plan postępowania z ryzykiem

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

§ 10 Szkolenia

1. Każdy użytkownik – przed dopuszczeniem do przetwarzania danych osobowych – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
2. Za przeprowadzenie szkolenia odpowiada Administrator, który może zlecić jego przeprowadzenie Inspektorowi Ochrony Danych lub podmiotowi zewnętrznemu, posiadającemu odpowiednią wiedzę i doświadczenie do jego przeprowadzenia.
3. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (zmiana sprzętu na sprzęt nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.

§ 11 Upoważnienia

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie. Wzór upoważnienia stanowi załącznik nr 2 do Polityki.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia

5. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Wzór ewidencji stanowi załącznik nr 3 do Polityki.

§ 12 Postępowanie upoważnionych użytkowników

1. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.
2. W tym celu należy:
   1) zwracać szczególną uwagę przy wchodzeniu i wychodzeniu z obiektu na podejrzane osoby lub samochody parkujące w pobliżu,
   2) przestrzegać procedur związanych z otwieranych i zamykaniem pomieszczeń, a także z wejściem do obszarów przestrzegania danych osobowych lub osób nieupoważnionych,
   3) informować Administratora, Inspektora Danych Osobowych lub pracowników ochrony

      o podejrzanych osobach tj.:
      a) osobach zachowujących się nienormalnie np. nieodpowiednio ubranych do pory roku, dnia i pogody;
      b) osobach przebywających w obiekcie bez wyraźnego celu;
      c) osobach posiadających przy sobie podejrzane bagaże, w których mogą być ukryte niebezpieczne przedmioty;
      d) przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy a także po jej zakończeniu.
3. Administrator, a także osoby na stanowiskach samodzielnych oraz użytkownicy zobowiązani są, na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Inspektorowi Danych Osobowych projekty i propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.

§ 13 Dostęp do pomieszczeń

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności co najmniej jednego użytkownika lub za zgodą Administratora Danych.
3. Zakaz wyrażony w ust. 2 dotyczy innych, niż określeni w ust. 1, pracowników Administratora Danych oraz pracowników służb technicznych, porządkowych, itp.

§ 14 Polityka kluczy

1. Klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu.
2. Klucze wydawane są wyłącznie osobom do tego uprawnionym, prowadzona jest ewidencja odbioru kluczy.
3. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych.

§ 15 Stosowane zabezpieczenia mające wpływ na ochronę danych osobowych

Administrator wdraża następujące środki mające na celu zapewnienie ochrony danych osobowych:

1. Środki organizacyjne:
   a) Opracowano i wdrożono politykę ochrony danych osobowych;
   b) Opracowano i wdrożono instrukcję zarządzania systemem informatycznym;
   c) Powołano Inspektora Ochrony Danych;
   d) Powołano Administratora Systemu Informatycznego;
   e) Do przetwarzania danych dopuszczono wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora Danych;
   f) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
   g) Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych;

h) Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy;
i) Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
j) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco;
k) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
l) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
m) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe. Wzór umowy powierzenia przetwarzania danych stanowi załącznik nr 4 do Polityki. Administrator prowadzi rejestr umów powierzenia przetwarzania danych osobowych, który stanowi załącznik nr 5 do Polityki;
n) W podmiocie prowadzi się politykę czystego biurka i ekranu;
o) W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe;
p) Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym;
q) Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

2. Środki ochrony fizycznej danych:
    a) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi, posiadającymi zamykane zamki, chyba, że z przepisów prawa wynika obowiązek stosowania drzwi spełniających dodatkowe wymagania techniczne np. drzwiami o podwyższonej odporności ogniowej >= 30 min, o podwyższonej odporności na włamanie - drzwi klasy C.
    b) Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna jeśli zlokalizowane na parterze zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
    c) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
    d) Dostęp do budynku, w którym znajdują się pomieszczenia, w których przetwarzany jest zbiór danych osobowych przez cała dobę jest nadzorowany przez służbę ochrony.
    e) Co do zasady zbiór danych osobowych w formie papierowej, prowadzony w formie kartoteki jest przechowywany w zamkniętej niemetalowej szafie, do których dostęp mają wyłącznie użytkownicy. W przypadku gdy wymaga tego przepis prawa zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej metalowej szafie, bądź w zamkniętym sejfie lub kasie pancernej.
    f) Kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętym sejfie lub kasie pancernej.
    g) Gdy wymaga tego szczegółowy przepis prawa, zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
    h) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
    i) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. W przypadku kartotek, po upływie okresu ich niezbędnej archiwizacji, wynikającego z instrukcji kancelaryjnej są niszczone przez podmiot zewnętrzny spełniający warunki prawidłowego wykonania usługi.

3. Opis zabezpieczeń infrastruktury informatycznej, w tym środki w ramach narzędzi programowych i baz danych zawiera instrukcja zarządzania systemami informatycznymi stanowiąca załącznik nr 6, do niniejszej polityki.

ROZDZIAŁ II
Przetwarzanie danych osobowych

§ 16 Miejsce i zasady przetwarzania danych

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, pomieszczeniach na terenie siedziby Administratora Danych.
2. Przetwarzanie danych osobowych w urządzeniach przenośnych może odbywać się poza obszarem przetwarzania danych, wyłącznie za zgodą Administratora Danych.
3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe zawiera załącznik nr 7 do Polityki.
4. Przetwarzanie, w tym udostępnianie danych osobowych, jest prawnie dopuszczalne, jeżeli jest to niezbędne dla realizowania uprawnienia lub spełniania obowiązku wynikającego z przepisu prawa.
5. Podmiot występujący o udostępnienie danych osobowych powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępniania. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne, i czy nie będzie ono stanowić naruszenia zasad ochrony danych osobowych.
6. Przetwarzanie, w tym udostępnianie danych osobowych, w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celach naukowych, dydaktycznych, historycznych lub statystycznych.
7. Udostepnienie danych osobowych może nastąpić jedynie za zgodą Administratora Danych lub osoby przez niego udostępnionej.

§ 17 Zabezpieczenie pomieszczeń

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić aby:

1. Drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby,
2. Budynek był chroniony przez wszystkie dni w roku. Ochronie powinny podlegać wyznaczone pomieszczenia w stopniu adekwatnym do ich przeznaczenia,
3. Pomieszczenia, w których znajdują się serwery, były wyposażone w miarę możliwości w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej,
4. Pracownicy Administratora Danych są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe.
5. Przebywanie użytkowanie po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych.
6. W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych osobowych jest zabronione.

§ 18 Inspektor Ochrony Danych Osobowych

1. Inspektor Danych Osobowych nadzoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych.
2. W celu sprawnego wykonywania swoich zadań Inspektor Ochrony Danych Osobowych jest uprawniony do wnioskowania do Administratora Danych w celu wyznaczania użytkownikom wykonywania określonych zadań.
3. Użytkownicy zobowiązani są do ścisłej współpracy z Inspektorem Danych Osobowych.

§ 19 Zakres przetwarzanych danych osobowych

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Wykaz zbiorów danych osobowych, których administratorem jest Administrator Danych oraz procesów przetwarzania zachodzących w tych zbiorach stanowi Załącznik nr 8 do Polityki.
3. Administrator Danych prowadzi:

3.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,

3.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.

4. Rejestr, o którym mowa w pkt 3.1. zawiera co najmniej następujące informacje:

4.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,

4.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,

4.3. imię i nazwisko oraz dane kontaktowe IOD,

4.4. cele przetwarzania,

4.5. opis kategorii osób, których dane dotyczą,

4.6. opis kategorii danych osobowych,

4.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

4.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

4.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

4.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

5. Rejestr, o którym mowa w pkt 3.2. zawiera co najmniej następujące informacje:

5.1. nazwę oraz dane kontaktowe Administratora Danych,

5.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,

5.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,

5.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,

5.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

5.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

5.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

6. Administrator Danych prowadzi rejestry, o których mowa w pkt 3 w formie elektronicznej. Wzory rejestrów, o których mowa w pkt 3 stanowią załącznik nr 12 i 13.

7. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

ROZDZIAŁ IV

Kontrola przestrzegania zasad zabezpieczenia ochrony danych osobowych

§ 20 Kontrola przestrzegania zasad ochrony danych osobowych

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, przynajmniej raz na rok.
2. Inspektor Danych Osobowych sprawuje nadzór nad przestrzeganiem zasad ochrony przetwarzania danych osobowych.
3. W przypadku nieobecności Inspektora Danych Osobowych, osobę zastępującą wyznacza Administrator Danych.
4. Inspektor Danych Osobowych lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
5. Inspektor Danych Osobowych prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.

6. Z kontroli, o których mowa w ust. 3 należy sporządzić dokument, które przechowuje Administrator Danych.

ROZDZIAŁ V

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 21 Czynności poprzedzające przystąpienie do pracy

1. Przed przystąpieniem do pracy użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora oraz Inspektora Ochrony Danych.
3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych.
4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemie informatycznym, jak i w kartotekach.

§ 22 Czynności podjęte po stwierdzeniu naruszenia

1. Do czasu przybycia Administratora lub Inspektora Ochrony Danych osobowych, zgłaszający:
   1) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
   2) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez umożliwienie dostępu do nich osobom nieupoważnionym,
   3) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych.

§ 23 Wstępne czynności po stwierdzeniu naruszenia

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Inspektor Ochrony Danych Osobowych, po przybyciu na miejsce:

1. Ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,
2. Wysłuchuje relacji osoby, która dokonała powiadomienia,
3. Podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia danych osobowych. W uzasadnionych przypadkach niezwłoczne powiadamia Administratora Danych.

§ 24 Raport z przebiegu zdarzenia

1. Inspektor Ochrony Danych Osobowych sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:
   1) Dacie i godzinie powiadomienia,
   2) Rodzaj naruszenia,
   3) Obowiązek zawiadomienia osoby, której dane dotyczą,
   4) Okoliczności naruszenia,
   5) Skutki naruszenia,
   6) Podjęte działania zaradcze,
2. Inspektor Ochrony Danych Osobowych sporządzony raport przekazuje do organu nadzorczego.

§ 25 Podjęcie czynności zmierzających likwidację naruszenia

1. Inspektor Ochrony Danych Osobowych podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
   1) W miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
   2) Relacjonuje Administratorowi Danych przedsięwzięte czynności,

3) O ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób dopuszczonych do przetwarzania danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, Inspektor Danych Osobowych wnioskuje do Administratora Danych o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec sprawcy/sprawców.

§ 26 Kontynuacja pracy

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia Inspektora Ochrony Danych Osobowych.

§ 27 Postępowanie w przypadku kradzieży

1. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Inspektora Ochrony Danych Osobowych, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
2. W sytuacji, o której mowa w ust. 1 Inspektor Ochrony Danych Osobowych podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt oraz powiadamia Administratora Danych.

§ 28 Odpowiedzialność

Osoba dopuszczona do przetwarzania danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki ponosi odpowiedzialność przewidzianą w przepisach aktów wewnętrznych Administratora Danych oraz na podstawie innych, odrębnych przepisów prawa.

§ 29 Zgłoszenie incydentu do UODO i obowiązek prowadzenia rejestru

1. Administrator przy współpracy z Inspektorem Ochrony Danych Osobowych jest zobowiązany zidentyfikować, ocenić i zgłosić naruszenie ochrony danych osobowych do Urzędu Ochrony Danych Osobowych w terminie 72 godzin od ustalenia naruszenia.

2. Administrator prowadzi wewnętrzny rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO. Wzór rejestru stanowi załącznik nr 9 do Polityki. Rejestr prowadzony jest w wersji elektronicznej.

ROZDZIAŁ VI
Postępowanie w przypadku klęski żywiołowej

§ 30 Definicja

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

§ 31 Zasady postępowania w przypadku ewakuacji

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 32 Obowiązek informacyjny

1. O zagrożeniu, jego skali i podjętych krokach zaradczych użytkownik zobowiązany jest niezwłocznie powiadomić Inspektora Ochrony Danych Osobowych w każdy możliwy sposób. w razie niemożności skontaktowania się z nim pracownik zawiadamia, co najmniej jedną z niżej wymienionych osób:
   1) Osobę wyznaczoną przez Administratora Danych,
   2) Administratora Danych.
2. Numery telefonów Inspektora Danych Osobowych i osób, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane użytkownikom.

§ 33 Prawo wejścia do pomieszczeń

Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełnienia obowiązku, o którym mowa w § 13 ust. 2 Polityki.

§ 34 Czynności poprzedzające opuszczenie pomieszczeń

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy – w miarę możliwości przed opuszczeniem tych pomieszczeń do:

1) Zamknięcia systemu informatycznego,
2) Zabezpieczenia danych gromadzonych w kartotekach.

§ 35 Zabezpieczenie danych

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Inspektor Danych Osobowej oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczyć dane osobowe przed nieupoważnionym do nich dostępem.
2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych , obecnych przy akcji ratunkowej.

ROZDZIAŁ VI
Postanowienia końcowe

§ 36 Poufność zapisów polityki

Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.

§ 37 Oświadczenie o dochowaniu poufności

1. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami Rozporządzeniu Parlamentu Europejskiego i Rady (UE) oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania oraz dochowania poufności.
2. Wzór oświadczenia potwierdzającego zaznajomienie użytkownika z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) oraz wydanych na jej podstawie aktów wykonawczych oraz dokumentacją obowiązującą u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania oraz dochowania poufności, stanowi załącznik nr 10 do polityki.
3. Oświadczenia przechowywane są w aktach osobowych.
4. Ponadto załącznik do niniejszej polityki stanowi wzór ogólnej klauzuli informacyjna – załącznik nr 11.

§ 38 Odpowiednie stosowanie innych przepisów

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) oraz wydanych na jej podstawie aktów wykonawczych.

2. Użytkownicy zobowiązani sia do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w przypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

……
(podpis Administratora Danych)