WÓJT GMINY
BIAŁOGARD
ul. Wileńska 8
78-200 Białogard

Zarządzenie Nr 71/2018
Wójta Gminy Białogard
z dnia 25 maja 2018 r.

w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Białogard" oraz „Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Białogard".

Na podstawie art. 33 ust. 1 i ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r., poz. 994 ze zm.) oraz § 3, § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024) zarządza się co następuje:

§ 1

Wprowadza się Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Białogard w brzmieniu stanowiącym załącznik nr 1 do niniejszego zarządzenia.

§ 2

Wprowadza się Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Białogard w brzmieniu stanowiącym załącznik nr 2 do niniejszego zarządzenia.

§ 3

Zobowiązuje się wszystkie osoby przetwarzające dane osobowe w Urzędzie Gminy Białogard do przestrzegania reguł zawartych w dokumentach wymienionych w § 1 i § 2.

§ 4

Traci moc zarządzenie Nr 45/2015 Wójta Gminy Białogard z dnia 30 czerwca 2015 r. w sprawie wprowadzenia „ Polityki Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard „ i „ Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Białogard".

§ 5

Zarządzenie wychodzi w życie z dniem podpisania.

WÓJT
Jacek Smoliński

RADCA PRAWNY
Waldemar Bleczyc
KO 354/91

Załącznik Nr 2 do Zarządzenia Wójta Gminy Białogard Nr 71/2018 z dnia 25 maja 2018 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

w Urzędzie Gminy Białogard

SPIS TREŚCI:

1. Odpowiedzialność za bezpieczeństwo przetwarzanych danych osobowych

W UG Białogard**wszyscy pracownicy** ponoszą **odpowiedzialność** za bezpieczeństwo przetwarzania danych osobowychzgodnie z posiadanymi zakresami obowiązków. **Każdy pracownikobowiązany jest** dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi, w tym m. in.:

1. Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych,
2. Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,
3. Zabezpieczyć sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione,
4. Utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia/zakończeniu umowy,
5. Stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z zasad ochrony danych osobowych,

2. Autoryzacja nowych informatycznych środków przetwarzania informacji

Każde nowe lub zmienione urządzenie, system informatyczny lub proces służący do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji, musi zostać zweryfikowane na zgodność z wymaganiami systemu ochrony danych osobowych i zaakceptowane przez ADO.

3. Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

Do przetwarzania danych osobowych dopuszczone mogą zostać tylko i wyłącznie osoby posiadające pisemne, imienne upoważnienia do przetwarzania danych osobowych.

Jeśli dana osoba ma przetwarzać dane osobowe w systemie informatycznym za pomocą urządzeń komputerowych, musi ona mieć przyznane imienne zabezpieczone hasłem konto w systemie informatycznym oraz nadane identyfikatory i prawa dostępu do poszczególnych aplikacji służących do przetwarzania danych osobowych.

Nadawanie uprawnień

Uprawnienia w systemie informatycznym służącym do przetwarzania danych osobowych nadaje ASI, na podstawie przekazanego upoważnienia do przetwarzania danych osobowych. Upoważnienie do przetwarzania danych osobowych określa zakres uprawnień do przetwarzania danych osobowych w tym przetwarzania wykonywanego w systemach informatycznych poprzez określenie poziomu uprawnień użytkownika w ramach systemu/systemów przetwarzających dane osobowe. Określenie poziomu uprawnień użytkownika wykonuje się poprzez określenie roli użytkownika w systemie, która opisuje

jego uprawnienia do korzystania z systemu informatycznego w procesie przetwarzania danych osobowych w UG.

W przypadku nowego użytkownika ASI tworzy konto użytkownika oraz rejestruje jego login i hasło, a następnie wprowadza do systemu uprawnienia użytkownika.

W przypadku modyfikacji uprawnień użytkownika, ASI odbiera wcześniej nadane uprawnienia i wprowadza do systemu nowe uprawnienia zgodnie z zakresem określonym w upoważnieniu do przetwarzania danych osobowych.

ASI prowadzi ewidencję pracowników oraz innych upoważnionych użytkowników zarejestrowanych w systemie informatycznym i przyznanych im uprawnień do systemu informatycznego służącego do przetwarzania danych osobowych.

Odbieranie uprawnień

Wyrejestrowania użytkownika z systemu informatycznego dokonuje ASI. Wyrejestrowanie może mieć charakter czasowy lub trwały. Wyrejestrowanie następuje poprzez:

1. zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
2. usunięcie danych użytkownika z bazy aktywnych (blokada konta) użytkowników systemu oraz odebranie uprawnień (wyrejestrowanie trwałe).

Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zaangażowany był użytkownik lub wygaśnięcie/wycofanie upoważnienia do przetwarzania danych osobowych.

Sposób zarządzania pozostałymi uprawnieniami użytkowników w systemie informatycznym

ASI w ramach wykonywania obowiązków odpowiedzialny jest także za zarządzanie uprawnieniami użytkowników w zakresie:

1. poziomu uprzywilejowania konta użytkownika w systemie operacyjnym stacji roboczej (lub w usłudze katalogowej),
2. dostępie do zasobów sieci Internet,
3. dostępie do przenośnych nośników danych.

W ramach tych uprawnień ASI jest zobowiązany, zgodnie z obowiązującą w UG BIAŁOGARDzasadą przydzielania użytkownikowi minimalnych uprawnień niezbędnych do wykonywania obowiązków służbowych, do

1. przydzielania użytkownikom konta w systemie operacyjnym stacji roboczej (lub w usłudze katalogowej) o poziomie dostępu użytkownik. Konta o poziomie administratora stacji roboczej (usługi katalogowej) może używać jedynie ASI. Dopuszcza się odstępstwo od tej reguły jedynie w przypadku pisemnej zgody ADO upoważniającej ASI do przydzielenia wskazanemu imiennie użytkownikowi uprawnień o poziomie administratora
2. blokowania użytkownikom dostępu do zasobów sieci Internet.
3. blokowania możliwości dostępu i użytkowania przenośnych nośników danych

Udzielenie użytkownikowi dostępu do zasobów sieci Internet może nastąpić jedynie za pisemną zgodą ADO.
Udzielenie użytkownikowi prawa dostępu i możliwości użytkowania przenośnych autoryzowanych nośników danych może nastąpić jedynie za pisemną zgodą ADO. ASI jest

zobowiązany w takim przypadku do aktualizacji dokumentacji użytkowników i nośników danych z zachowaniem zasad rozliczalności i identyfikacji użytkownika oraz nośnika danych.

4. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

System informatyczny wyposażony jest w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu. Podstawowym elementem umożliwiającym dostęp do systemu jest login użytkownika oraz hasło, które jest wykorzystywane do weryfikowania tożsamości użytkownika.

Użytkownik systemu jest **zobowiązany** do **zarządzania swoimi hasłami** oraz **zachowania poufności haseł.**

Niedopuszczalne jest ujawnianie i przekazywanie swojego identyfikatora wraz z hasłem innym osobom, jak również niedopuszczalne jest pracowanie w systemie, aplikacji lub programie na koncie innego użytkownika.

Niedopuszczalne jest udostępnianie stanowiska komputerowego, programu lub aplikacji innym osobom po zalogowaniu się na swoim koncie. Użytkownik udostępniający stanowisko komputerowe innemu upoważnionemu Użytkownikowi zobowiązany jest do wcześniejszego wylogowania się z aplikacji i systemu.

Jedynym akceptowalnym odstępstwem od tej zasady jest udostępnienie stanowiska ASI, jeśli ten w ramach obowiązków służbowych musi wykonać czynności w systemie informatycznym, dla których niezbędna jest praca w kontekście konta danego użytkownika i wymagająca wykonania tych czynności jako dany użytkownik /np. bieżąca pomoc użytkownikowi, konfiguracja systemu lub aplikacji/. Obowiązkiem pracownika w takim przypadku, jest pozostanie przy stanowisku, obserwacja i kontrola działań ASI. W pozostałych przypadkach ASI jest zobowiązany do wykonywania działań w kontekście własnego imiennego konta, które zapewnia mu uprawnienia administracyjne w stosunku do kont innych użytkowników.

Każdy z użytkowników posiada dostęp tylko do tych systemów, zasobów informatycznych i funkcji aplikacji, które są mu niezbędne do wykonywania obowiązków służbowych. Próby nieautoryzowanego dostępu do innych funkcji aplikacji i systemów lub jakichkolwiek zasobów informatycznych mogą zostać potraktowane jako świadome naruszenie zasad bezpieczeństwa systemów informatycznych.

Zarządzanie hasłami użytkowników

Hasła użytkowników przydziela ASI w sposób zapewniający zachowanie poufności hasła oraz informuje użytkownika o obowiązku zmiany hasła na własne przy pierwszym logowaniu;

Hasło powinno składać się z unikalnego zestawu **co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.** Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

System informatyczny wymusza okresową zmianę hasła; administrator bezpieczeństwa informacji może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

Użytkownik **ponosi pełną i absolutną odpowiedzialność** za użycie zasobów informatycznych Urzędu przy wykorzystaniu jego hasła do momentu powiadomienia administratora systemu o ujawnieniu hasła. Obowiązkiem użytkownika jest natychmiastowa

zmiana hasła i niezwłoczne powiadomienia ASI oraz IOD w każdym przypadku zaistnienia podejrzenia, że hasło zostało ujawnione innemu użytkownikowi lub osobom trzecim.

Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

W przypadku systemów dostępnych przez przeglądarkę internetową - zabrania się użytkownikom zachowywania (zapamiętywania) wprowadzanych loginów i haseł w formularzach logowania przeglądarki internetowej.

Zarządzanie hasłami administratorów

- Administratorów systemu obowiązują wszelkie zasady dotyczące użytkowników
- Istotne dla działania systemu teleinformatycznego hasła objęte są specjalną ochroną. Przechowywane są one w sposób bezpieczny w pomieszczeniu administratora systemu, w metalowych szafach lub sejfie. Miejsce przechowywania zdeponowanych haseł powinno być zabezpieczone przed dostępem osób nieuprawnionych oraz przed zniszczeniem w wyniku działania czynników zewnętrznych.
- Dostęp do zdeponowanych haseł posiada ASI oraz ADO. W przypadku wystąpienia sytuacji awaryjnej ADO może zdecydować o przekazaniu hasła innemu uprawnionemu użytkownikowi, należy zapewnić rozliczalność użycia haseł w sytuacji awaryjnej oraz odnotować przekazanie hasła.

5. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przetwarzanych w systemie informatycznym przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

Obowiązkiem każdego użytkownika systemu jest zapewnienie, że żadna inna osoba nie ma możliwości obserwowania klawiatury w czasie procedury logowania, gdy wprowadzane jest indywidualne hasło dostępu. Zabronione jest współużytkowanie hasła dostępu i przydzielonego konta z innymi osobami. Po zalogowaniu użytkownik jest odpowiedzialny za zapewnienie, że stacja komputerowa nie zostanie pozostawiona bez opieki, dostępna dla innych użytkowników, aż do chwili wylogowania z systemu.

Niedopuszczalne jest ujawnianie i przekazywanie swojego identyfikatora wraz z hasłem innym osobom, jak również niedopuszczalne jest pracowanie w systemie, aplikacji lub programie na koncie innego użytkownika.

Niedopuszczalne jest udostępnianie stanowiska komputerowego, programu lub aplikacji innym osobom po zalogowaniu się na swoim koncie. Pracownik udostępniający stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązany jest do wcześniejszego wylogowania się z aplikacji i systemu.

Przetwarzając dane osobowe w systemie informatycznym użytkownik zobowiązany jest do wykonania czynności mających na celu zapewnienie bezpieczeństwa przetwarzanych danych:

1. ustawić monitory komputerów w sposób uniemożliwiający osobom nieupoważnionym podgląd ekranu i/lub stosować filtry prywatyzujące,
2. uaktywnić wygaszacz ekranu chroniony hasłem w czasie zawieszenia pracy trwającego dłużej niż 10 min lub w sytuacjach, gdy osoba nieuprawniona może mieć możliwość podglądu ekranu monitora,
3. stosować politykę czystego ekranu
4. stosować politykę czystego biurka

Polityka czystego ekranu

Polityka czystego ekranu ma na celu zabezpieczenie przed nieautoryzowanym dostępem do systemów teleinformatycznych i zabezpieczenie przez ujawnieniem informacji chronionych.

Każdorazowe odejście od stanowiska pracy powinno **zostać poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu** tak, aby niemożliwe było uzyskanie do niego nieautoryzowanego dostępu. Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wylogować się z systemu lub też zablokować dostęp do systemu.

Użytkownik blokuje dostęp do systemu operacyjnego poprzez naciśnięcie klawiszy Ctrl+Alt+Delete oraz kliknięcie w „Zablokuj komputer" (lub skrótem klawiaturowym: Logo Windows + L). Do wyłączenia blokady niezbędne jest podanie hasła użytkownika.

Polityka czystego biurka

W celu zapobiegania nieautoryzowanemu dostępowi do danych osobowych lub kradzieży informacji i środków jej przetwarzania UG Białogard stosuje politykę czystego biurka.

Chronione dokumenty i nośniki danych nie mogą pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pomieszczeniu służbowym. Pomieszczenie należy zamknąć w sposób uniemożliwiający dostęp dla osób nieuprawnionych. Po zakończeniu pracy dokumenty i komputerowe nośniki z danymi przechowywane są w szafach, a pomieszczenia zamykane zgodnie z obowiązującymi w UG BIAŁOGARDzasadami

Procedura rozpoczęcia pracy

1. Przed przystąpieniem do pracy z systemem, użytkownik zobowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest niezwłocznie powiadomić o tym fakcie IOD oraz ASI i stosować się do otrzymanych od nich wytycznych.

3. Rozpoczynając pracę na komputerze, pracownik musi podać wszystkie wymagane, własne identyfikatory i hasła, w sposób uniemożliwiający ich ujawnienie innym osobom.

4. Pracownik zobowiązany jest uwierzytelniać się w systemie informatycznym, wyłącznie na podstawie **własnego** identyfikatora i hasła. Uwierzytelnienie lub próby uwierzytelniania przy pomocy identyfikatorów i haseł innych pracowników będą traktowane jako świadome naruszenie zasad bezpieczeństwa systemów informatycznych.

5. Każdy z pracowników posiada dostęp tylko do tych funkcji aplikacji, które są mu niezbędne w codziennej pracy. Próby nieautoryzowanego dostępu do innych funkcji aplikacji lub jakichkolwiek zasobów informatycznych będą traktowane jako świadome naruszenie zasad bezpieczeństwa systemów informatycznych.

6. W przypadku braku możliwości zalogowania się pracownika do działającego systemu informatycznego lub dostępu do funkcjonalności systemu, niezbędnych do realizacji zadań służbowych, należy poinformować ASI.

Wszystkie stanowiska komputerowe działające w systemie informatycznym urzędu powinny posiadać uaktywnioną opcję wygaszacza ekranu w przypadku braku aktywności użytkownika w systemie. **Czas uaktywnienia wygaszacza ekranu nie może być dłuższy niż 10 minut**. Odblokowanie wygaszacza ekranu wymaga podania hasła. System umożliwia uaktywnienie wygaszacza ekranu na żądanie użytkownika.

Procedura zawieszenia pracy

W sytuacji gdy użytkownik zmuszony jest opuścić stanowisko komputerowe poza zajmowane pomieszczenie lub kiedy wgląd do danych wyświetlanych na ekranie monitora może mieć nieuprawniona osoba, należy bezwzględnie skorzystać z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu chronionego hasłem. Hasło wygaszacza ekranu jest zbieżne z hasłem logowania do systemu.

W przypadku opuszczenia stanowiska pracy na krótki czas należy zawiesić pracę w systemie i zablokować konsolę systemu przez naciśnięcie CTRL+ALT+DEL i wciśnięcie przycisku „Zablokuj Komputer" (lub skrótem klawiaturowym: Logo Windows + L).

Po powrocie do swojego stanowiska pacy należy odblokować konsolę podając hasło.

W przypadku opuszczenia stanowiska pracy na dłuższy okres czasu należy zapisać dane, zakończyć pracę w aplikacji lub systemie i następnie wylogować się z systemu.

Procedura zakończenia pracy

Kończąc pracę, użytkownik obowiązany jest do:

1) wylogowania się z aplikacji i systemu, a następnie wyłączenia sprzętu komputerowego;

2) zabezpieczenia stanowiska pracy, w szczególności schowania do zamykanych szaf, szuflad itp.

wszelkiej dokumentacji oraz przenośnego sprzętu komputerowego i nośników magnetycznych, optycznych i papierowych (**zasada „czystego biurka"**).

6. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania.

Obowiązki ASI

W systemie informatycznym **kopie zapasowe tworzy ASI**. Tworzy się kopie zapasowe zbiorów danych oraz programów i narzędzi służących do ich przetwarzania.

Dopuszcza się powierzenie czynności wykonywania i przechowywania kopii bezpieczeństwa innym podmiotom pod warunkiem podpisania umowy powierzenia przetwarzania danych osobowych w ustalonym zakresie.

ASI w porozumieniu z IOD opracowuje oraz utrzymuje aktualny spis aktywów (systemów informatycznych, baz danych, plików, plików konfiguracyjnych i inne) podlegających procedurze wykonywania kopii zapasowych.

ASI w porozumieniu z IOD sporządza harmonogram wykonywania kopii zapasowych.

ASI przed dokonaniem istotnych zmian konfiguracyjnych w systemie informatycznym mogących skutkować niestabilnym działaniem systemu (np. aktualizacja systemu, zmiany konfiguracji) jest zobowiązany do wykonania dodatkowej kopii bezpieczeństwa niezależnie od przyjętego harmonogramu wykonywania kopii zapasowych.

Kopie zapasowe należy umieszczać na nośnikach zewnętrznych typu zewnętrzne dyski twarde lub dyski sieciowe, taśmy streamera (DDS, DAT) i stosować się do zaleceń producenta nośnika w odniesieniu do czasu jego eksploatacji.

Zaleca się przechowywanie kopii bezpieczeństwa poza lokalizacją/pomieszczeniem w którym znajduje się system informatyczny dla którego wykonuje się kopię bezpieczeństwa.

Dostęp do kopii bezpieczeństwa mają wyłącznie ASI , uprawniony personel informatyczny firmy zewnętrznej oraz IOD.

Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/tygodniowa/miesięczna" wraz z podaniem daty sporządzenia.

ASI odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego. Po odtworzeniu systemu informatycznego ASI odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.

ASI przeprowadza weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych.

Czynność odtworzenia danych nie może spowodować zagrożenia utraty poufności, utraty, nadpisania lub zmiany danych przetwarzanych w środowisku produkcyjnym; weryfikację przeprowadza się w środowiskach testowych lub dane odtwarza się do alternatywnej lokalizacji w systemie plików.

Weryfikacja powinna być przeprowadzana nie rzadziej niż raz na pół roku.

ASI w celach dowodowych dokumentuje przeprowadzenie czynności weryfikacji oraz jej rezultat.

ASI prowadzi rejestr, w którym odnotowuje błędy wykonania kopii bezpieczeństwa oraz awaryjne i okresowe (wykonywane w ramach weryfikacji) odtworzenia kopii bezpieczeństwa.

Obowiązki użytkowników

Zobowiązuje się użytkowników systemu informatycznego Urzędu**do zapisywania plików zawierających dane osobowe (w szczególności danych osobowych w formie elektronicznej przetwarzanych przy użyciu narzędzi pakietów biurowych MS Office lub innych)** oraz innych ważnych zasobów **na dysku sieciowym zapewniającym bezpieczeństwo danych –według zaleceń ASI.**

7. Procedury i okres przechowywania nośników informacji zawierających dane osobowe oraz kopii zapasowych

Zbiory danych przechowywane są na serwerach obsługujących system informatyczny administratora danych.

Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych oraz ich przesyłania pocztą elektroniczną odbiorcom bez uprzedniego zaszyfrowania.

W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym.

Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

Nośniki zawierające dane osobowe przeznaczone do likwidacji pozbawia się wcześniej tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający odczytanie danych.

Nośniki zawierające dane osobowe przeznaczone do naprawy pozbawia się wcześniej tych danych albo naprawia się je pod nadzorem ASI.

8. Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

Na działanie wirusów komputerowych i innego szkodliwego oprogramowania narażone są wszystkie stanowiska komputerowe, które są przyłączone do sieci komputerowej oraz te, które są wyposażone w czytniki nośników elektronicznych (takich jak stacje dyskietek, czytniki optyczne i inne nośniki danych umożliwiające wprowadzenie danych lub programów z zewnątrz) lub interfejsy komunikacyjne pozwalające na podłączanie do systemu takich urządzeń (np. złącza USB, interfejsy WIFI, Bluetooth lub inne).
Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

- załączniki do poczty elektronicznej,
- przeglądane strony internetowe,
- pliki i aplikacje pochodzące z sieci publicznej lub nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

Zabezpieczenie informacji/systemów/sieci przed wirusami, programami szpiegującymi oraz złośliwym oprogramowaniem realizuje się poprzez stosowanie następujących zasad i wdrożenie zabezpieczeń:.

1. Stosowanie oprogramowania antywirusowego na wszystkich stacjach roboczych i serwerach systemu
2. Ochronę połączenia internetowego urzędu.
3. Kontrolowanie i monitorowanie dostępu do zasobów sieci publicznych (Internetu).
4. Instalację i aktywację zapór sieciowych (firewall) na wszystkich systemach i na styku połączeń pomiędzy siecią lokalną i sieciami publicznymi.
5. Aktywację zapór sieciowych na każdej stacji roboczej i serwerze.
6. Uaktualnianie systemów operacyjnych i programów.
7. Sporządzanie kopii zapasowych ważnych danych/informacji biznesowych.
8. Szkolenie pracowników w zakresie podstawowych zasad bezpieczeństwa danych.

Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerze, stacjach roboczych oraz komputerach przenośnych przez administratora systemu.

Oprogramowanie antywirusowe, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerem i stacjami roboczymi.

Niezależnie od ciągłego nadzoru, ASI okresowo przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerze i stacjach roboczych.

Do obowiązków ASI należy zapewnienie aktualizacji oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji.

Do obowiązków ASI należy konfiguracja oprogramowania antywirusowego w sposób zapewniający:

1. Uniemożliwienie użytkownikom odinstalowania, wyłączenia ochrony stacji roboczych oraz obniżenie poziomu ochrony oprogramowania antywirusowego
2. Wysyłanie powiadomień do ASI o każdym wykrytym przez system antywirusowy incydencie związanym ze szkodliwym oprogramowaniem

Obowiązki użytkowników

Użytkownik jest obowiązany zawiadomić administratora systemu o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu

zawartości nośnika oprogramowaniem antywirusowym.

ASI, za zgodą ADO, blokuje lub zezwala na możliwość wykorzystywania w systemie informatycznym zewnętrznych nośników danych typu pamięci usb (pendrive), karty pamięci, dyski zewnętrzne oraz urządzeń umożliwiających składowanie danych typu smartfony, tablety.

Połączenie z sieci publicznych do wewnętrznych systemów teleinformatycznych musi odbywać się poprzez komunikację zaszyfrowaną.

Połączenia pomiędzy lokalnymi sieciami znajdującymi się w różnych lokalizacjach (budynkach) jednostki muszą być realizowane poprzez komunikację szyfrowaną.

Zabrania się użytkownikom:

1. pobierać, uruchamiać (w tym aplikacji przenośnych ang. portable) i instalować na sprzęcie służbowym jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonuje ASI.
2. przyłączać i użytkować prywatnego sprzętu, w tym prywatnych nośników danych lub urządzeń pozwalających nawiązywać połączenie z Internetem (modemów lub urządzeń typu smartfon tablet, umożliwiających nawiązanie połączenia) bez wyraźnej i udokumentowanej zgody ADO
3. korzystać z dostępu do Internetu w celach pozasłużbowych
4. przechowywać na sprzęcie służbowym gier oraz plików multimedialnych np. filmów, obrazów ,dźwięków nie związanych z zadaniami służbowymi
5. podejmować jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją

9. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych

Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym administratora danych przeprowadzane są przez ASI lub przez personel zewnętrzny za zgodą ADO i pod nadzorem ASI

Naprawy i zmiany w systemie informatycznym administratora danych przeprowadzane przez serwisanta prowadzone są pod nadzorem administratora systemu informatycznego w siedzibie administratora danych, (jeśli to możliwe) lub poza siedzibą administratora danych, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, **a jeśli wiązałoby się to z nadmiernymi utrudnieniami, po podpisaniu umów powierzenia przetwarzania danych osobowych.**

Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie.

10. Zasady korzystania z komputerów przenośnych zawierających dane osobowe

Użytkownicy, którym zostały powierzone komputery przenośne, zobowiązani są chronić je przed uszkodzeniem lub utratą, szczególną ostrożność należy zachować podczas ich przenoszenia i transportu.

Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.

Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to administratorowi systemu informatycznego.

Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację wykazuje automatycznie system oraz zapory sieciowe

Komputery przenośne zabezpiecza się poprzez wprowadzenie **zabezpieczeń kryptograficznych** polegających na **szyfrowaniu dysku twardego urządzenia**, blokowanie zbędnych portów i interfejsów komunikacyjnych oraz uniemożliwienie załadowania systemu operacyjnego z innego niż dysk twardy nośnika danych.

11. Dokumentacja bezpieczeństwa systemu

ASI prowadzi elektroniczny system ewidencji:

1. sprzętu komputerowego i nośników danych,
2. użytkowników pracujących w systemie,
3. nadanych uprawnień użytkownikom do właściwych systemów informatycznych,
4. miejsc przetwarzania danych osobowych,
5. kopii bezpieczeństwa,
6. systemów/aplikacji administrowanych przez Urząd oraz administrowanych przez inne podmioty
7. systemów informatycznych, w których przetwarzane są dane osobowe, zawierający opis struktury zbiorów danych, pól informacyjnych i ich wzajemnych powiązaniach oraz sposób przepływów danych pomiędzy poszczególnymi systemami.

W przypadku prowadzenia ewidencji w formie elektronicznej należy zabezpieczyć ją poprzez okresowe wykonywanie kopii zapasowej. Ewidencje sprzętu komputerowego mogą być prowadzone również w formie papierowej.

12. Postanowienia końcowe

W sprawach nieokreślonych niniejszą instrukcją należy stosować przepisy RODO, ustawy o ochronie danych osobowych oraz instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć oświadczenie, potwierdzające znajomość treści instrukcji.

Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.

Załącznik Nr 1 do Zarządzenia Wójta Gminy Białogard Nr 71/2018 z dnia 25 maja 2018 r.

Polityka Bezpieczeństwa Informacji

w Urzędzie Gminy Białogard

1. Wstęp

Celem niniejszego dokumentu jest opisanie zasad ochrony osób fizycznych w związku z przetwarzaniem danych osobowych wdrożonych w **Urzędzie Gminy Białogard**, zwanym dalej **UGBiałogard.**

Stosownie do naczelnej zasady określonej w RODO wyrażonej w postaci poszanowania i ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, Administrator – Gmina Białogard, reprezentowana przez Wójta Gminy Białogard, kierując się konstytucyjnymi i ustawowymi zadaniami wprowadza do powszechnego stosowania regulacje odpowiedniej ochrony przedmiotowych praw.

Administrator w trybie art. 24 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. Zastosowane środki w razie potrzeby poddawane są przeglądom i uaktualniane odpowiednio do zmian przepisów prawa oraz potrzeb placówki .

Administrator – w trybie art. 37 ust. 1 lit. a RODO i art. 7 UODO, wyznaczył Inspektora Ochrony Danych Osobowych, na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, prawa oświatowego, charakterystyki działań placówki oświatowej oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

Polityka Bezpieczeństwa Informacji odnosi się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych w formie tradycyjnych nośników jak i danych przetwarzanych w systemach informatycznych administratora, a także przez podmioty przetwarzające w imieniu Administratora.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano wszystkie obowiązki leżące po stronie administratora danych, podając jednocześnie procedury postępowania w określonych sytuacjach.

Na niniejszą dokumentację składają się: Polityka Bezpieczeństwa Informacji oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zestawienia informacji uzupełniających treść dokumentu zebrano w postaci załączników. **Wypełnione załączniki podlegają ścisłej ochronie.** Zabrania się publikowania niniejszej dokumentacji w Internecie.

Podstawowym celem Polityki Bezpieczeństwa Informacji (PBI), jest organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych w odpowiednich dla potrzeb kategoriach przetwarzania danych, w tym także w zgodności z zasadami zapewniającymi integralność, poufność i rozliczalność oraz systematyczne edukowanie użytkowników systemu ochrony danych osobowych. PBI jest jednocześnie dokumentem określającym zadania pracowników, a także podmiotów współpracujących, w zakresie właściwej legalności przetwarzania danych.

Celem Polityki jest m. in.:
1. Wprowadzenie jednolitej formy ochrony danych osobowych w obszarze działania UG Białogard.

Polityka Bezpieczeństwa Informacji

w Urzędzie Gminy Białogard

1. Wstęp

Celem niniejszego dokumentu jest opisanie zasad ochrony osób fizycznych w związku z przetwarzaniem danych osobowych wdrożonych w **Urzędzie Gminy Białogard**, zwanym dalej **UGBiałogard.**

Stosownie do naczelnej zasady określonej w RODO wyrażonej w postaci poszanowania i ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, Administrator – Gmina Białogard, reprezentowana przez Wójta Gminy Białogard, kierując się konstytucyjnymi i ustawowymi zadaniami wprowadza do powszechnego stosowania regulacje odpowiedniej ochrony przedmiotowych praw.

Administrator w trybie art. 24 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. Zastosowane środki w razie potrzeby poddawane są przeglądom i uaktualniane odpowiednio do zmian przepisów prawa oraz potrzeb placówki .

Administrator – w trybie art. 37 ust. 1 lit. a RODO i art. 7 UODO, wyznaczył Inspektora Ochrony Danych Osobowych, na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, prawa oświatowego, charakterystyki działań placówki oświatowej oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

Polityka Bezpieczeństwa Informacji odnosi się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych w formie tradycyjnych nośników jak i danych przetwarzanych w systemach informatycznych administratora, a także przez podmioty przetwarzające w imieniu Administratora.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano wszystkie obowiązki leżące po stronie administratora danych, podając jednocześnie procedury postępowania w określonych sytuacjach.

Na niniejszą dokumentację składają się: Polityka Bezpieczeństwa Informacji oraz Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zestawienia informacji uzupełniających treść dokumentu zebrano w postaci załączników. **Wypełnione załączniki podlegają ścisłej ochronie.** Zabrania się publikowania niniejszej dokumentacji w Internecie.

Podstawowym celem Polityki Bezpieczeństwa Informacji (PBI), jest organizacyjne, fizyczne i logiczne zabezpieczenie posiadanych danych osobowych w odpowiednich dla potrzeb kategoriach przetwarzania danych, w tym także w zgodności z zasadami zapewniającymi integralność, poufność i rozliczalność oraz systematyczne edukowanie użytkowników systemu ochrony danych osobowych. PBI jest jednocześnie dokumentem określającym zadania pracowników, a także podmiotów współpracujących, w zakresie właściwej legalności przetwarzania danych.

Celem Polityki jest m. in.:

1. Wprowadzenie jednolitej formy ochrony danych osobowych w obszarze działania UG Białogard.
2. Wskazanie działań i reguł postępowania w zakresie ochrony danych osobowych.
3. Zapewnienie rozliczalności uczestników przetwarzania danych w zakresach lub czynnościach określonych indywidualnymi upoważnieniami użytkowników.
4. Zachowanie poufności przetwarzanych danych osobowych w określonych przepisami granicach prawa.
5. Nadzorowanie procesów przetwarzania danych w określonych ustawą i przepisami resortowymi przesłankach przetwarzania.
6. Ustawowe nadzorowanie procesu przetwarzania danych przez dostawców usług.

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych stosuje się następujące zasady:

- „**przywilejów koniecznych**" – każdy pracownik posiada uprawnienia ograniczone wyłącznie do tych, które są mu niezbędne i konieczne do wykonywania powierzonych mu obowiązków służbowych;
- „**wiedzy koniecznej**" – każdy pracownik posiada dostęp do danych osobowych ograniczony wyłącznie do tych, które są mu niezbędne i konieczne do wykonywania powierzonych obowiązków służbowych;
- „**indywidualnej odpowiedzialności**" – każdy pracownik powinien mieć jednoznacznie określony zakres indywidualnej odpowiedzialności za przetwarzane dane osobowe;
- „**czystego biurka**" – zabronione jest pozostawianie na stanowisku pracy jakichkolwiek dokumentów lub nośników zawierających dane osobowe po zakończeniu dnia pracy lub w trakcie czasowej nieobecności.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych przez AD do przetwarzania danych osobowych, zarówno zatrudnionych (bez względu na rodzaj stosunku pracy), jak i innych wykonujących obowiązki na rzecz UG, np. praktykantów, stażystów, wolontariuszy.

2. Przepisy Prawa

1. Rozporządzenie 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), *Dz. U. UE . L. 2016.119.1*z dnia 4 maja 2016r.
2. Konstytucja Rzeczypospolitej Polskiej z dnia 02 kwietnia 1997 r. (Dz. U. z 1997r., Nr 78 poz. 483 ze zm.) - art. 47 i 51
3. Ustawa z dnia 26.04.1974 r. Kodeks pracy
4. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000)
5. Rozporządzenie Rady Ministrów z 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

3. ODPOWIEDZIALNOŚĆ DYSCYPLINARNA I KARNA

Za naruszenie wymogów niniejszej Dokumentacji, naruszenie zasad i trybu przetwarzania danych oraz obowiązku ich zabezpieczenia każdy pracownik podlega odpowiedzialności dyscyplinarnej Niezależnie od tego, zgodnie z przepisami karnymi ustawy dnia 10 maja 2018 r. o ochronie danych osobowych, naruszenie jej przepisów jest zagrożone w następujący sposób:

Przepisy karne
Art. 107. [Nielegalne przetwarzanie danych osobowych]

1. Kto **przetwarza** dane osobowe, choć ich **przetwarzanie nie jest dopuszczalne** albo **do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.**

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech**.

Art. 108. [Udaremnianie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych]
Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Administracyjne kary pieniężne
Art. 102. [Nałożenie administracyjnej kary pieniężnej na jednostki sektora finansów publicznych, instytuty badawcze lub NBP]

1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:
1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;

2) instytut badawczy;

3) Narodowy Bank Polski.

2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

3. Administracyjne kary pieniężne, o których mowa w ust. 1 i 2, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

4. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. **Administrator (AD)** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
   W UG Białogard obowiązki ustawowe administratora danych wypełnia Wójt Gminy Białogard.

2. **Administrator systemu informatycznego(ASI)** – należy przez to rozumieć wykonawcę lub wyznaczoną osobę realizującą czynności nadzoru użytkowników, systemów w obszarze informatyki w zgodności z PBI oraz obowiązującymi przepisami prawa.

3. **Analiza ryzyka** - systematyczne monitorowanie postępowania użytkowników w obszarach przetwarzania danych, analiza i ocena przepisów prawa w kontekście dokonania koniecznych zmian zachodzących w posiadanych systemach informatycznych, stacjach roboczych i urządzeniach mobilnych. Analiza obejmuje także sprawdzenie wiedzy użytkowników w przedmiotowym zakresie.

4. **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji w jednostce, z gwarantowanym zakresem dostępu użytkowników, realizowane poprzez systematyczny nadzór i aktualizację wewnętrznych przepisów prawa w zgodności z ogólnymi przepisami prawa i regulacjami resortowymi.

5. **Dane osobowe** - oznaczają 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

6. **Dane szczególne** – określone jako szczególny rodzaj informacji osobowych, ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby
   1) **dane genetyczne** - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej

2) **dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne
3) **dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia

7. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym Urzędu, stanowiący klucz uprawnionego dostępu do konkretnych urządzeń i danych.

8. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu, nadany przez AD.

9. **Incydent związany z bezpieczeństwem informacji** - jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań statutowych i zagrażają bezpieczeństwu gromadzonych i zabezpieczanych informacji.

10. **Inspektor Ochrony Danych Osobowych(IODO)** – należy przez to rozumieć wykonawcę lub osobę wyznaczoną przez Wójta gminy Białogard, w zgodności z treścią art. 37 ust. 1 lit. a RODO oraz art. 8 UODO, do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów prawa o ochronie danych osobowych.

11. **Naruszenie ochrony danych osobowych** - oznacza 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

12. **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 zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania

13. **Ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

14. **PBI** – Polityka Bezpieczeństwa Informacji, dokumentacja zatwierdzona przez Wójta, do stosowania w UGBiałogard.

15. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

16. **Poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom

17. **Prezes Urzędu Ochrony Danych Osobowych** – oznacza krajowy organ nadzorczy w rozumieniu RODO i UODO

18. **Przetwarzanie** – 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
19. **RODO** - Rozporządzenie 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),*Dz. U. UE . L. 2016.119.1*z dnia 4 maja 2016r.

20. **Rozporządzenie KRI**- Rozporządzenie Rady Ministrów z 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016, poz. 113)

21. **Strona trzecia** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe

22. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

23. **UODO** - USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000)

24. **Uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu

25. **Użytkownik** - pracownik lub inna osoba upoważniona przez Administratora do przetwarzania danych osobowych na jego polecenie, w formie tradycyjnej i elektronicznej.

26. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem, nadzorowany przez IOD i ASI

27. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

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

W Urzędzie zgody wymagają działania na danych osobowych, wykraczające poza ustawową delegację przetwarzania ***(zgody na uczestniczenie w konkursach, publikacją wizerunku na stronach www, profilach w mediach społecznościowych, gazetkach i tablicach informacyjnych)***. Zgoda, jest deklaracją określoną czasem i zakresem przetwarzania danych, możliwą do wycofania w dowolnym czasie. W działalności urzędu występują dwa rodzaje zgody, po pierwsze zgoda na przetwarzanie danych zwykłych w związku z czynnościami wykraczającymi poza granice ustawowej dyspozycji, a także w przypadku danych szczególnych kategorii przekazywanych w trakcie rekrutacji pracowniczej oraz w szczególnych przypadkach organizowanych wydarzeń i imprez. W trybie określonym ustawą, zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

5. Cel i zakres polityki

Przepisy RODO wymagają aby dane osobowe przetwarzane były w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Celem niniejszej Polityki Bezpieczeństwa jest opracowanie zgodnych z wymogami prawa i optymalnych zasad przetwarzania danych, których zbieranie i przetwarzanie jest niezbędne dla realizacji obowiązków i zadań ustawowych i statutowych UG Białogard oraz dla bieżącej działalności Urzędu.

W Urzędzie Gminy Białogard są przede wszystkim dane osobowe mieszkańców gminy, interesantów, petentów, pracowników, wnioskodawców, korespondentów oraz osób współpracujących na podstawie umów cywilnoprawnych. UG Białogard, w związku z realizacją zadań, przetwarza także między innymi dane osobowe kontrahentów i kandydatów do pracy, uczestników imprez i wydarzeń organizowanych przez UG oraz osób biorących udział w sesjach Rady Gminy .

6. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

W celu poprawnej realizacji postanowień niniejszej Polityki wprowadza się poniższy **zakres ról i odpowiedzialności** w zakresie zapewnienia właściwego procesu zarządzania bezpieczeństwem przetwarzanych danych osobowych.

Odpowiedzialność za bezpieczeństwo danych osobowych ponosząwszyscy pracownicy i współpracownicy Urzędu Gminy Białogard zgodnie z zakresami obowiązków i upoważnieniami wydanymi przez AD.

DANE OSOBOWE MOGĄ PRZETWARZAĆ OSOBY WYŁĄCZNIE NA POLECENIE ADMINISTRATORA POSIADAJĄCE ODPOWIEDNIE UPOWAŻNIENIE NADANE PRZEZ AD

ADMINISTRATOR DANYCH OSOBOWYCH (AD)

Administrator Danych Osobowych realizuje zadania w zakresie ochrony przetwarzanych danych osobowych, w tym zwłaszcza:

1. podejmuje decyzje o celach i środkach przetwarzania danych osobowych, zwłaszcza z uwzględnieniem zmian w obowiązującym prawie, organizacji UG oraz technik zabezpieczania danych osobowych;
2. prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych,
3. uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z obowiązującym prawem;
4. nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
5. upoważnia poszczególne osoby do przetwarzania danych osobowych w stosownym, indywidualnie określonym zakresie;

6. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych;
7. zatwierdza wzory dokumentów dotyczących ochrony danych osobowych przygotowywane przez komórki organizacyjne;
8. wyznacza IOD, publikuje jego dane kontaktowe i zawiadamia o nich organ nadzorczy w terminie 14 dni od dnia wyznaczenia wskazując dane zawarte w art. 10 ustawy;
9. zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
10. wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej;
11. zapewnia, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań;
12. bez zbędnej zwłoki- w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza organowi nadzorczemu naruszenia ochrony danych osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
13. jeżeli ww. naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu;
14. dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze,
15. jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych,
16. jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

INSPEKTOR OCHRONY DANYCH (IOD)

Inspektor ochrony danych jest wyznaczany przez Administratora Danych. IOD może być członkiem personelu administratora lub wykonywać zadania na podstawie umowy o świadczenie usług.

Inspektor ochrony danych osobowych realizuje poniższe zadania z zakresu ochrony danych osobowych:

1. informuje ADO, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradza im w tej sprawie;
2. monitoruje przestrzeganie RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania

zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. nadzór nad prowadzeniem i przechowywaniem rejestru wydanych upoważnień;
4. w przypadku naruszenia przepisów RODO albo niniejszej Polityki niezwłocznie informuje ADO o naruszeniu i postępuje zgodnie z przepisami RODO;
5. udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie zgodnie z art. 35 RODO;
6. współpracuje z organem nadzorczym;
7. pełni funkcje punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacje we wszelkich innych sprawach

IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. IOD może wykonywać inne zadania i obowiązki, jeżeli nie powodują one konfliktu interesów. Nie jest on odwoływany ani karany przez administratora za wypełnianie swoich zadań. IOD bezpośrednio podlega najwyższemu kierownictwu administratora. Osoby, których dane dotyczą, mogą kontaktować się IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO (ASI)

Administrator systemu informatycznego bezpośrednio odpowiada za zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych, a w szczególności:

1. zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
2. zobowiązany jest do systematycznego kontrolowania i testowania bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
3. zobowiązany jest do cyklicznego przeprowadzania audytów w obszarze wybranych procedur bezpieczeństwa danych osobowych;
4. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
5. przydziela każdemu upoważnionemu użytkownikowi identyfikator oraz hasło do systemu informatycznego, przydział następuje na pisemny wniosek bezpośredniego przełożonego użytkownika;
6. nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
7. podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu w systemie informatycznym;
8. wyrejestrowuje użytkowników oraz zmienia zakresy uprawnień na polecenie ADO;
9. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ADO o naruszeniu i współdziała z nim przy usuwaniu jego skutków;
10. prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;

11. nadzoruje wykonywanie napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe;
12. sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
13. przydziela i rejestruje służbowe komputerowe nośniki informacji.
14. współpracuje z IOD w zakresie koordynacji zaleceń IOD i przepływu informacji pomiędzy IOD i osobami upoważnionymi
15. przechowuje oraz zabezpiecza dokumentację bezpieczeństwa systemów IT i dokumenty powiązane

PRACOWNIK DZIAŁU KADR- stanowisko ds. organizacyjnych, kadrowych i wydawania dowodów tożsamościORK

1. Przedkłada ADO do podpisu upoważnienia do przetwarzania danych osobowych
2. Przedkłada pracownikowi upoważnienia do przetwarzania danych osobowych
3. W porozumieniu z IOD dokonuje unieważnienia upoważnienia poprzez umieszczenie stosownej daty ustania na upoważnieniu oraz w ewidencji danych osobowych, a także poprzez ustne poinformowanie osoby, której upoważnienie wygasło.
4. W porozumieniu z IOD prowadzi aktualną ewidencji osób upoważnionych do przetwarzania danych
5. Przedstawia do podpisu pracownikowi upoważnionemu do przetwarzania danych osobowych zobowiązania do zachowania w tajemnicy tych danych osobowych oraz sposobów ich zabezpieczenia
6. Informuje IOD oraz ASI o zatrudnieniu, zamianie zakresu obowiązków lub stanowiska, zwolnieniu oraz długotrwałej nieobecności pracowników/współpracowników UG
7. Współpracuje z IOD w zakresie koordynacji zaleceń IOD i przepływu informacji pomiędzy IOD i osobami upoważnionymi
8. Przechowuje oraz zabezpiecza dokumentację bezpieczeństwa i dokumenty powiązane (Rejestr Czynności Przetwarzania, Wykazy, Analizy ryzyka i inne)

PRACOWNIK/WSPÓŁPRACOWNIK PRZETWARZAJĄCY DANE OSOBOWE

Każda osoba przetwarzająca dane osobowe (pracownik, współpracownik, bezpośredni przełożony, samodzielne stanowisko) **ma obowiązek**:

1.) znać podstawy prawne, na jakich dokonuje konkretnych czynności przetwarzania danych osobowych;

2.) sprawowania kontroli nad wprowadzaniem i udostępnianiem danych osobowych;

3.) nadzorowania fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe oraz kontroli przebywających w nich osób;

4.) niezwłocznego informowania Administratora oraz Inspektora Ochrony Danych i ASI o przypadkach naruszenia przepisów o ochronie danych osobowych.

5.) dbać o bezpieczeństwo przetwarzanych danych osobowych oraz przetwarzać dane osobowe w sposób zgodny z przepisami RODO, Ustawy ,Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.

6.) zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia

PERSONEL SPRZĄTAJĄCY

Obowiązki pracowników personelu sprzątającego w sytuacji natknięcia się na dokumenty lub nośniki danych mogących zawierać dane osobowe w trakcie wykonywania obowiązków poza godzinami pracy urzędu lub pod nieobecność osoby upoważnionej do przetwarzania danych:

Przerwać wykonywanie dalszych czynności w danym pomieszczeniu. Zabezpieczyć pomieszczenie. Powiadomić pracownika działu kadr.

7. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, zbiorów danychoraz systemów IT

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

Wzór wykazu stanowi załącznik Nr 1 do Polityki Bezpieczeństwa
Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych prowadzi IOD. Zestawienie zbiorów przechowuje pracownik działu kadr.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych jednostki organizacyjnej w postaci dokumentów papierowych i w systemie informatycznym, w którym stosowane są pakiety biurowe lub wyspecjalizowane aplikacje (programy).
Zestawienie zbiorów danych osobowych oraz programów do przetwarzania tych danych prowadzi IOD. Zestawienie zbiorów przechowuje pracownik działu kadr.

Wzór wykazu zbiorów stanowi załącznik Nr 2 do Polityki bezpieczeństwa.

Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do przekazywania IOD informacjio zamiarze utworzenia nowego zbioru danych osobowych oraz o zmianach w zbiorach już istniejących.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

1. Obiegdokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi jednostki , winien się odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).
2. Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną jednostki odbywa się w relacji jednostka organizacyjna - mieszkańcy, przedsiębiorcy, kontrahenci, zakład ubezpieczeń społecznych, urząd skarbowy, banki, Narodowy Fundusz Ochrony Zdrowia, urząd wojewódzki, urząd marszałkowski inne jednostki administracji samorządowej i rządowej.
3. Zabronione jest jednoczesne podłączanie komputerów do sieci wewnętrznej Urzędu Gminy Białogard i sieci zewnętrznych (Plus , Era , Orange , Play, pozostałe sieci komórkowe, WiFi , WiMAX itp.).
4. ASI prowadzi wykaz sposobu przepływu danych pomiędzy poszczególnymi systemami, wzór stanowi załącznik Nr 4 do Polityki bezpieczeństwa.

8. Rejestr Czynności przetwarzania

W UG prowadzony jest w zgodności z art. 30 RODO Rejestr czynności przetwarzania danych osobowychoraz Rejestr kategorii czynności przetwarzania.

Rejestry prowadzi IOD w porozumieniu z osobami uczestniczącymi w danych czynnościach przetwarzania.

9. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

A) Zabezpieczenia organizacyjne

1. Został wyznaczony IOD
2. Została opracowana i wdrożona polityka bezpieczeństwa
3. Została opracowana i wdrożona instrukcja zarządzania systemem informatycznym
4. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych
5. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych
6. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony osób fizycznych i danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego
7. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
8. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
9. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych lub za wyraźną zgodą Administratora oraz w warunkach zapewniających bezpieczeństwo danych
10. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe

B) Zabezpieczenia ochrony fizycznej danych osobowych

Kontrola dostępu osób do obszaru przetwarzania danych osobowych, na poziomie zabezpieczenia pomieszczeń.

Stosowanie polityki czystego biurka i polityki czystego ekranu

Ochrona budynku przez stosowanie zamknięć i systemów alarmowych oraz zabezpieczanie budynku poza godzinami pracy UG

C) Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

D) Zabezpieczenia narzędzi programowych i baz danych

Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

10. Podstawowe zasady ochrony danych osobowych.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do ochrony danych osobowych na swoim stanowisku pracy jak i poza nim, w przypadku przetwarzania danych osobowych, do których posiada upoważnienie w innych lokalizacjach, zgodnie z zasadami określonymi w niniejszej Polityce oraz w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w dokumentach z nimi powiązanych, tj. innych aktów wewnętrznie obowiązujących w jednostce z zakresu ochrony danych osobowych.
2. Osoby wykonujące czynności związane z przetwarzaniem danych osobowych zobowiązane są do zabezpieczenia materiałów zawierających dane osobowe w sposób uniemożliwiający nieuprawnione ujawnienie danych, nieautoryzowany dostęp, niedozwolone: powielenie, modyfikację, zniszczenie, utratę, nieprawidłowe wykorzystanie lub kradzież.
3. Osoby mające dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w zakresie wykraczającym poza wykonywanie obowiązków służbowych.
4. Przekazywanie danych w ramach wewnętrznej struktury jednostki może następować wyłącznie pomiędzy osobami posiadającymi upoważnienie do przetwarzania danych osobowych w określonym zbiorze i zakresie.
5. W pomieszczeniach, w których przetwarzane są dane osobowe, przebywać mogą wyłącznie osoby upoważnione do przetwarzania tych danych osobowych. Osoby nieposiadające odpowiedniego upoważnienia do przetwarzania danych osobowych mogą przebywać w obszarze przetwarzania danych wyłącznie w obecności osoby upoważnionej lub na podstawie zgody Administratora Danych.
6. Dokumenty zawierające dane osobowe winny być przechowywane w szafach zamykanych na klucz. Niedopuszczalnym jest pozostawianie kluczy w zamkach pod nieobecność osoby nieupoważnionej, w szczególności po zrealizowaniu czynności służbowych w danym dniu pracy.
7. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zabezpieczania przed dostępem osób nieuprawnionych wszelkich pomieszczeń, w których przetwarzane są dane osobowe. W szczególności osoby takie zobowiązane są do zamykania tych pomieszczeń na klucz, jeżeli opuszczają je jako ostatni.
8. Klucze do pomieszczeń, w których przetwarzane są dane osobowe, mogą pozostawać w dyspozycji jedynie właściwych osób upoważnionych.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej oraz z wykorzystaniem nośników elektronicznych pracownicy zobowiązani są do nie pozostawiania materiałów zawierających dane osobowe w miejscach umożliwiających fizyczny dostęp do nich osobom nieuprawnionym.
10. Każdy dokument papierowy zawierający dane osobowe sporządzony jako dokument roboczy należy najpóźniej na koniec dnia pracy zniszczyć lub zamknąć w miejscu uniemożliwiającym dostęp osób nieuprawnionych.
11. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe winno się odbywać w sposób uniemożliwiający odczytanie zawartej w nich treści.

12. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz bezpośredni przełożony pracownika.
13. Kopiowanie danych osobowych utrwalonych w postaci papierowej bądź elektronicznej może odbywać się wyłącznie przez osobę w ramach posiadanego przez nią upoważnienia do przetwarzania danych osobowych, w związku z realizacją czynności służbowych.
14. Szczegółowe uregulowania w zakresie zasad bezpieczeństwa obowiązujących przy przetwarzaniu danych w systemach informatycznych, z wykorzystaniem poczty elektronicznej oraz w związku z użytkowaniem sprzętu elektronicznego zawarte są w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

11. Instrukcja postępowania w sytuacji naruszenia ochrony danych

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik Urzędu Gminy Białogard w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego, ASI oraz IOD.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, 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, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia zagrożenia, ASI oraz IOD prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości

d. dokumentuje prowadzone postępowania

5. W przypadku stwierdzenia incydentu (naruszenia), IOD prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
    b. zabezpiecza ewentualne dowody
    c. ustala osoby odpowiedzialne za naruszenie
    d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
    e. inicjuje działania dyscyplinarne
    f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości
    g. dokumentuje prowadzone postępowania
    h. powiadamia AD o konieczności notyfikacji naruszenia organowi nadzorczemu (Prezesowi UODO) lub powiadomienia osób, których dane dotyczą
6. IOD jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
    - zgłoszenia od pracowników
    - wiedza IOD
    - wyniki kontroli
7. W przypadku, gdy IOD stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną
8. IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
9. Po przeprowadzeniu działań korygujących lub zapobiegawczych, IOD jest zobowiązany do oceny efektywności ich zastosowania.

12. Postanowienia końcowe

1. „Polityka Bezpieczeństwa" jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią „Polityki bezpieczeństwa" każdego użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce".
5. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Białogard

WYKAZ POMIESZCZEŃ STANOWIĄCYCH OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

Wykaz lokalizacji/pomieszczeń w których dopuszczalne jest przetwarzanie danych osobowych. Przetwarzanie danych osobowych może odbywać się w specjalnie przygotowanych i zabezpieczonych pomieszczeniach we wskazanych lokalizacjach:

Budynek Urzędu Gminy Białogard ul. Wileńska 8, 78-200 Białogard		
L.P.	**Nazwa pomieszczenia**	**Miejsce ,położenie**
1.	Gabinet Wójta	pokój nr 16
2.	Gabinet Zastępcy Wójta/Sekretarz	pokój nr 16
3.	Sekretariat	pokój nr 16
4.	Ewidencja ludności i dowodów osobistych Radca prawny	pokój nr 8
5.	Podatki	pokój nr 12
6.	Archiwum	pokój - piwnica
7.	Ewidencja Działalności Gospodarczej	pokój nr 17
8.	Biuro Rady	pokój nr17
9.	Serwerownia	pom. - piwnica

Załącznik Nr 2 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

Wykaz zbiorów danych przetwarzanych w Urzędzie Gminy Białogard

Lp	NAZWA ZBIORU	Zakres przetwarzanych w zbiorze danych o osobach	Inne dane osobowe	System danych T-tradyc. I-inform.	Nazwa Programu 1) forma danych 2) zabezpieczenie informatyczne, 3) bazę danych chroni UPS (TAK / NIE)	Lokalizacja	Zabezpieczenie fizyczne
1.	TYTUŁY WYKONAWCZE	Nazwiska i imiona, imiona rodziców, data urodzenia, PESEL, adres zamieszkania lub pobytu,	NIP, REGON, miejsce pracy, zawód, numer telefonu	I	Gmina2 1) osobowe 2) uwierzytelnianie - login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 12	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
2.	EWIDENCJA PODATNIKÓW I DZIERŻAWCÓW NIERUCHOMOŚCI	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL,	NIP, REGON, numer telefonu, nazwa i adres siedziby	I	Gmina2 1) osobowe 2) uwierzytelnienie - login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 12, 13	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
3.	EWIDENCJA PŁATNIKÓW OPŁAT	Nazwiska i imiona, adres zamieszkania lub pobytu	----------	I	Gmina2 1) osobowe 2) uwierzytelnienie - login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 12	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
4.	REJESTR PŁATNIKÓW OPŁAT ZA GOSPODAROWANIE ODPADAMI	Imię, nazwisko, adres nieruchomo ścina której powstają odpady komunalne, adres korespondencyjny, numer ewidencyjny PESEL,	NIP, numer telefonu	I	GOMIG 1) osobowe 2) uwierzytelnienie - login, hasło	Urząd Gminy Białogard ul. Wileńska 8,	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na

	KOMUNALNYMI				3) TAK	78-200 Białogard, pok. 7	klucz
5.	REJESTR KORESPONDENCJI PRZYCHODZACEJ	Nazwiska i imiona, adres zamieszkania lub pobytu	Numer telefonu	I	e-KANCELARIA 1) osobowe 2) uwierzytelnienie - login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
6.	SYSTEM INFORMACJI OŚWIATOWEJ	Imię i nazwisko, numer PESEL, data urodzenia,	Wykształcenia, miejsce pracy, zawód	I	SIO 1) osobowe 2) uwierzytelnienie - login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 17	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
7.	REJESTR MIESZKAŃCÓW I REJESTR ZAMIESZKANIA CUDZOZIEMCÓW	Nazwisko i imię, imiona, nazwisko rodowe, imiona i nazwiska rodowe rodziców, data urodzenia, miejsce urodzenia, kraj urodzenia, numer PESEL, stan cywilny, płeć, oznaczenie aktu urodzenia i urzędu stanu cywilnego w którym został on sporządzony, obywatelstwo albo status bezpaństwowca, imię i nazwisko rodowe małżonka oraz numer PESEL małżonka, jeżeli został mu nadany, data zawarcia związku małżeńskiego, oznaczenie aktu małżeństwa i urzędu stanu cywilnego w którym został on sporządzony, adres i data zameldowania na pobyt stały, kraj miejsca zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z miejsca pobytu stałego, adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu, data wymeldowania z miejsca pobytu czasowego, data wyjazdu poza granice RP trwającego dłużej niż 6		I	SELWIN 1) osobowe 2) uwierzytelnienie – login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 8	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz

	KOMUNALNYMI				3) TAK	78-200 Białogard, pok. 7	klucz
5.	REJESTR KORESPONDENCJI PRZYCHODZACEJ	Nazwiska i imiona, adres zamieszkania lub pobytu	Numer telefonu	I	e-KANCELARIA 1) osobowe 2) uwierzytelnienie - login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
6.	SYSTEM INFORMACJI OŚWIATOWEJ	Imię i nazwisko, numer PESEL, data urodzenia,	Wykształcenia, miejsce pracy, zawód	I	SIO 1) osobowe 2) uwierzytelnienie - login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 17	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
7.	REJESTR MIESZKAŃCÓW I REJESTR ZAMIESZKANIA CUDZOZIEMCÓW	Nazwisko i imię, imiona, nazwisko rodowe, imiona i nazwiska rodowe rodziców, data urodzenia, miejsce urodzenia, kraj urodzenia, numer PESEL, stan cywilny, płeć, oznaczenie aktu urodzenia i urzędu stanu cywilnego w którym został on sporządzony, obywatelstwo albo status bezpaństwowca, imię i nazwisko rodowe małżonka oraz numer PESEL małżonka, jeżeli został mu nadany, data zawarcia związku małżeńskiego, oznaczenie aktu małżeństwa i urzędu stanu cywilnego w którym został on sporządzony, adres i data zameldowania na pobyt stały, kraj miejsca zamieszkania, kraj poprzedniego miejsca zamieszkania, data wymeldowania z miejsca pobytu stałego, adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu, data wymeldowania z miejsca pobytu czasowego, data wyjazdu poza granice RP trwającego dłużej niż 6		I	SELWIN 1) osobowe 2) uwierzytelnienie – login, hasło 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 8	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz

		miesięcy i wskazanie kraju wyjazdu, data powrotu z wyjazdu poza granice RP trwającego dłużej niż 6 miesięcy, seria, numer i data ważności ostatniego wydanego dowodu osobistego obywatela polskiego oraz oznaczenie organu wydającego dokument, seria, numer i data ważności ostatniego paszportu, seria, numer i data ważności dokumentu podróży cudzoziemca, data zgonu , numer aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony					
8.	EWIDENCJA DOWODÓW OSOBISTYCH	Nazwisko, imię, imiona, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, PESEL, seria i numer dowodu osobistego,	Płeć, wizerunek twarzy, obywatelstwo, numer telefonu, adres e-mail,	I	SYSTEM REJESTRÓW PAŃSTWOWYCH ZRÓDŁO - RDO 1) osobowe 2) uwierzytelnienie login (karta chipowa), hasło, 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 8	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
9.	CENTRALNA EWIDENCJA DZIŁALNOŚCI GOSPODARCZEJ	Nazwisko i imię, adres, imiona rodziców, data urodzenia, miejsce urodzenia, PESEL, seria i nr dowodu osobistego	NIP, REGON	I	CEIDG 1) osobowe 2) uwierzytelnienie - login, hasło, podpis kwalifikowany 3) TAK	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. 17	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
10.	EWIDENCJA KORESPONDENCJI WYCHODZĄCEJ	Nazwiska i imiona, adres zamieszkania lub pobytu,	Numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
11.	REJESTR UPOWAŻNIEŃ I PEŁNOMOCNICTW	Nazwisko i imię, seria i nr dowodu osobistego, Nr ewidencyjny PESEL		T	Nie dotyczy	Urząd Gminy Białogard	Alarm, zamki patentowe, wydruki przechowywane

						ul. Wileńska 8, 78-200 Białogard, pok. Nr 8	w szafach zamykanych na klucz
12.	REJESTR ZAMÓWIEŃ PUBLICZNYCH	Nazwisko i imię, adres zamieszkania lub pobytu	Miejsce pracy, numer telefonu, fax, NIP, REGON	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
13.	EWIDENCJA POZWOLEŃ NA ROZBIÓRKĘ OBIEKTÓW BUDOWLANYCH	Nazwiska i imiona, adres zamieszkania lub pobytu,	Numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
14.	EWIDENCJA POZWOLEŃ NA BUDOWĘ	Nazwiska i imiona, adres zamieszkania lub pobytu,	Numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
15.	REJESTR DECYZJI CELU PUBLICZNEGO	Nazwiska i imiona, adres zamieszkania lub pobytu,	Numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
16.	REJESTR WYROBÓW ZAWIERAJACYCH AZBET	Nazwiska i imiona, adres zamieszkania lub pobytu	Numer identyfikacji podatkowej, numer REGON, numer telefonu,	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
17.	REJESTR WYDAWANYCH DECYZJI O ŚRODOWISKOWYCH UWARUNKO-WANIACH	Nazwiska i imiona, adres zamieszkania lub pobytu	Numer identyfikacji podatkowej, numer REGON, numer telefonu,	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz

18.	REJESTR ZEZWOLEŃ NA ODBIÓR ODPADÓW KOMUNALNYCH OD WŁAŚCICIELI NIERUCHOMOŚCI I OPRÓŻNIANIE ZBIORNIKÓW BEZODPŁYWOYCH	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL	Numer identyfikacji podatkowej, numer REGON, numer telefonu,	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
19.	REJESTR ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH	Nazwiska i imiona, adres zamieszkania lub pobytu, numer	Numer identyfikacji podatkowej, numer telefonu,	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
20.	REJESTR ZEZWOLEŃ NA USUWANIE DRZEW I KRZEWÓW	Nazwiska i imiona, adres zamieszkania lub pobytu, numer	numer telefonu,	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 6	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
21.	REJESTR PODATNIKÓW PODATKÓW OD SPADKÓW I DAROWIZN	Nazwiska i imiona, adres zamieszkania lub pobytu		T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 13	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
22.	OŚWIADCZENIA MAJATKOWE RADNYCH	Nazwiska i imiona, data urodzenia, miejsce urodzenia,	Zawód	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 17	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
23.	REJESTR DECYZJI O WARUNKACH ZABUDOWY	Nazwiska i imiona, adres zamieszkania lub pobytu	Numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
24.	REJESTR SKARG I	Nazwiska i imiona, adres	Numer telefonu	T	Nie dotyczy	Urząd Gminy	Alarm, zamki patentowe,

		dowodu osobistego				78-200 Białogard, pok. Nr 6	klucz
31.	REJESTR INNYCH OBIEKTÓW, W KTÓRYCH ŚWIADCZONE SĄ USŁUGI HOTELARSKIE	Nazwisko i imię, adres zamieszkania,	Nazwa przedsiębiorcy, nazwa własna obiektu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
32.	WYBORY ŁAWNIKÓW	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania, PESEL,	Zawód, numer identyfikacji podatkowej, miejsce pracy, zawód, wykształcenie	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 17	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
33.	REJESTR INFORMACJI PUBLICZNEJ	Nazwisko i imiona, adres zamieszkania,	Nazwa telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
34.	DOFINANSOWANIE PRACODOWCOM KOSZTÓW KSZTAŁCENIA PRACOWNIKÓW	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania, PESEL	Miejsce pracy, zawód, wykształcenie, numer identyfikacji podatkowej	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
35.	AWANS ZAWODOWY NAUCZYCIELI	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania	Miejsce pracy, zawód, wykształcenie	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 16	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
36.	EWIDENCJA OPŁAT ADIACENCKICH	Nazwiska i imiona, adres zamieszkania lub pobytu	Numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
37.	EWIDENCJA	Nazwiska i imiona, adres	Numer telefonu	T	Nie dotyczy	Urząd Gminy	Alarm, zamki patentowe,

	NUMERÓW PORZĄDKOWYCH NIERUCHOMOŚCI	zamieszkania lub pobytu				Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	wydruki przechowywane w szafach zamykanych na klucz
38.	EWIDENCJA ŚWIADCZEŃ OSOBISTYCH I RZECZOWYCH NA RZECZ SIŁ ZBROJNYCH	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu,	Miejsce pracy, zawód, numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 19	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
39.	REJESTR DO KWALFIKACJI WOJSKOWEJ	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, data urodzenia	Stanowisko\funkcja	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 19	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
40.	EWIDENCJA OŚWIADCZEŃ MAJATKOWYCH PRACOWNIKÓW	Nazwiska i imiona, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego	----------	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 8	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
41.	ZBIÓR DANYCH OSOBOWYCH ARCHIWUM	Nazwiska i imiona, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, seria i numer dowodu osobistego	Numer Identyfikacji Podatkowej, miejsce pracy, zawód, wykształcenie, numer telefonu	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. PIWNICA	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
42.	REJESTR DANYCH OSOBOWYCH "PLANOWANIE PRZESTRZENNE"	Nazwiska i imiona, adres zamieszkania lub pobytu,	----------	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8, 78-200 Białogard, pok. Nr 10	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na klucz
43.	REJESTR POZWOLEŃ WODNO-PRAWNYCH	Nazwiska i imiona, adres zamieszkania lub pobytu,	----------	T	Nie dotyczy	Urząd Gminy Białogard ul. Wileńska 8,	Alarm, zamki patentowe, wydruki przechowywane w szafach zamykanych na

Załącznik nr 3 do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

STRUKTURA ZBIORÓW

WZÓR

L.P.	NAZWA ZBIORU	ZAKRES DANYCH W ZBIORZE
1.	SYSTEM INFORMACJI OŚWIATOWEJ	✓ PESEL ✓ Płeć ✓ Wykształcenie ✓ nazwa szkoły i rok ukończenia ✓ warunki zatrudnienia ✓ staż pracy ✓ historia pracy, ✓ kary, nagrody ✓ tytuł zawodowy ✓ zawód wyuczony i wykonywany ✓ uzyskane kwalifikacje ✓ nieobecności w pracy

Załącznik nr4do Polityki Bezpieczeństwa w Urzędzie Gminy Białogard

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

WZÓR

LP.	Rodzaj urządzenia	Rodzaj zbioru	Docelowy system informatyczny	Zakres przesyłanych danych osobowych	Sposób transmisji
1.	KOMPUTER STACJONARNY, WINDOWS, UWIERZYTELNIANIE: IDENTYFIKATOR + HASŁO	Dokumentacja związana z	Word / Excel	• imię i nazwisko • data i miejsce urodzenia, • PESEL, • adres zamieszkania /zameldowania/	manualny
2.	KOMPUTER STACJONARNY, WINDOWS, UWIERZYTELNIANIE: IDENTYFIKATOR + HASŁO	System Informacji Oświatowej	SIO, uwierzytelnianie: identyfikator + hasło	• imię i nazwisko • data i miejsce urodzenia, • PESEL, • adres zamieszkania /zameldowania	przesyłanie danych poprzez sieć telekomunikacyjną