Polityka Ochrony Danych Osobowych

Powiat Czarnkowsko – Trzcianecki

Starostwo Powiatowe w Czarnkowie

2024

Cel:

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Podstawy prawne:

1. rozporządzenie Parlamentu Europejskiego i Rady Europy (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 (RODO) (4.5.2016, L 119);
2. ustawa z dnia 21 lutego 2019 r.o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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. 2019 poz. 730);
3. ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018 r., poz. 1000 z późn. zm.).

Przedmiot:

Przedmiotem Polityki ochrony danych osobowych są zasady i tryb postępowania podczas przetwarzania danych osobowych w formie tradycyjnej i elektronicznej. Mając na względzie obowiązek stosowania odpowiednich zabezpieczeń przetwarzanych danych osobowych w odniesieniu do zakresu, kontekstu i celu, a także ryzyka naruszenia ochrony przetwarzanych danych, zgodnie z art. 32 RODO, wdraża się odpowiednie środki techniczne i organizacyjne.

Zakres stosowania:

Polityka ochrony danych osobowych obowiązuje wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informacyjne, w których przetwarzane są dane osobowe. Politykę tę stosuje się we wszystkich lokalizacjach, w których przetwarzane są informacje podlegające ochronie, na wszystkich nośnikach informacji (tradycyjnych - papierowych, elektronicznych, optycznych, magnetycznych), które zawierają dane podlegające ochronie. Polityka obowiązuje wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, w tym stażystów i osób, z którymi podpisane są umowy cywilno-prawne wykonujących prace na rzecz Administratora oraz innych osób mających dostęp do danych.

Zatwierdzam i polecam stosować
Starosta Czarnkowsko-Trzcianecki

SPIS TREŚCI

Polityka Ochrony Danych Osobowych 1
Cel: 2
Podstawy prawne: 2
Przedmiot: 2
Zakres stosowania: 2
DEFINICJE 5
POSTANOWIENIA OGÓLNE 6
INSPEKTOR OCHRONY DANYCH I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH 6
OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH 7
REALIZACJA PRAW PRZEZ OSOBY, KTÓRYCH DANE DOTYCZĄ 9
OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH 10
ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI 11
POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH 11
POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH 13
PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM 14
POLITYKA HASEŁ 14
PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM 15
ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ 16
ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET) 17
ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH 17
UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH 18
KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ 19
OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM 19
POSTANOWIENIA KOŃCOWE 19
Załączniki 20/27 stronach: 20
Załącznik nr 1 Zgoda na przetwarzanie danych osobowych .. **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 2 Upoważnienie nr _____ do przetwarzania danych osobowych **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 3 Upoważnienie nr _____ do przebywania w obszarze przetwarzania danych osobowych..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 4 Odwołanie upoważnienia do przetwarzania danych osobowych/przebywania w obszarze przetwarzania tych danych..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 5 Ogólna klauzula informacyjna ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 6 Klauzula informacyjna dot. przetwarzania danych osobowych w związku z ustawą z dnia29 sierpnia 1997 r. - Ordynacja podatkowa).... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 7 Klauzula dot. debaty nad raportem o stanie powiatu - zgłoszenie chęci zabrania głosu..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 8 Klauzula dot. debaty nad raportem o stanie powiatu – lista poparcia mieszkańców ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 9 Klauzula informacyjna dot. skarg i wniosków . **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 10 Klauzula informacyjna dot. zdjęć/filmów upublicznianych przez Starostwo Powiatowe w Czarnkowie ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 11 Klauzula informacyjna dot. Rzecznika Konsumentów . **Błąd! Nie zdefiniowano zakładki.** Załącznik nr 12 Klazula informacyjna - Kandydaci do pracy .. **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 13 Klauzula informacyjna - Zatrudnieni ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 14 Klauzula informacyjna - Zamówienia publiczne i zaopatrzenie ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 15 Klauzula informacyjna o przetwarzaniu danych osobowych w celu realizacji zadań z zakresu ewidencji i oznaczania pojazdów ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 16 Klauzula informacyjna o przetwarzaniu danych osobowych do wydawania zezwoleń, licencji i zaświadczeń związanych z transportem drogowym ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 17 Wykaz incydentów powodujących naruszenie ochrony danych osobowych ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 18 Karta zgłoszenia do systemu * ..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 19 Raport z naruszenia ochrony danych osobowych..... **Błąd! Nie zdefiniowano zakładki.**

Załącznik nr 20 Instrukcja szyfrowania plików/katalogów przy pomocy narzędzia 7-Zip. **Błąd! Nie zdefiniowano zakładki.**

DEFINICJE

Ilekroć w niniejszej Polityce jest mowa o:

1. Administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych, a w niniejszej Polityce Starosta Powiatu Czarnkowsko-Trzcianeckiego z siedzibą Starostwa Powiatowego w Czarnkowie przy ul. Rybaki 3, 64-700 Czarnków, zwanego „Administratorem";
2. Inspektor Ochrony Danych (lub IOD) – rozumie się przez to osobę wyznaczoną przez Administratora, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami prawa;
3. Administratorze Systemów Informatycznych (lub ASI) – rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane przepisami prawa;
4. Danych osobowych (lub danych) – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5. Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;
6. Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;
7. Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska oraz stanowiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
8. RODO - Rozporządzenia 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 – RODO);
9. PUODO lub Urząd nadzoru – Prezes Urzędu Ochrony Danych Osobowych;
10. Zbiorze danych – rozumie się przez to dane zebrane w postaci zbioru lub według kategorii:
    a) danych osobowych klientów i kontrahentów Starostwa Powiatowego z podzbiorami,
    b) danych pracowniczych z podzbiorami,
    c) danych administracyjnych z podzbiorami,
    d) danych doraźnych,

przy czym każdy zbiór danych to zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE

§ 1.

Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1. Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy
3. Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi
6. Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, co nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań

INSPEKTOR OCHRONY DANYCH I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

§ 2.

1. Administrator wyznacza i zgłasza do rejestru prowadzonego przez Urząd nadzoru Inspektora Ochrony Danych, który jest odpowiedzialny za ich przetwarzanie.
2. Administrator wyznacza Administratora Systemów Informatycznych
3. Administrator wyznacza osoby współdziałając z IOD w zakresie ochrony danych osobowych.

§ 3.

W przypadku niewyznaczenia IOD lub ASI za zapewnienie należytego przestrzegania zasad ochrony danych osobowych odpowiada Administrator.

§ 4.

1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IOD z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez IOD odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotyczy należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 5.

Do przetwarzania danych osobowych w Starostwie Powiatowym w Czarnkowie są dopuszczone wyłącznie osoby upoważnione przez Administratora Danych Osobowych.

§ 6.

1. Upoważnienia nadawane są indywidualnie, przed dostępem do danych oraz rozpoczęciem przez osobę upoważnianą przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy oraz osoby fizyczne współpracujące z Administratorem, które uzyskają dostęp do danych osobowych w związku ze świadczeniem na jego rzecz usług na podstawie umów cywilnoprawnych lub jako osoby fizyczne wykonujące obowiązki na podstawie jednoosobowej działalności (zatrudnieni).
3. Upoważnienie nadawane jest niezwłocznie po przyjęciu do pracy lub po zawarciu umowy cywilnoprawnej, w sytuacjach, gdy zakres wykonywanych obowiązków wiąże się z potrzebą uzyskania dostępu do danych osobowych.
4. Upoważnienie nadawane jest na czas zatrudnienia na danym stanowisku pracy lub na czas realizacji zleconych czynności.
5. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Administratora.
6. Osoba posiadająca upoważnienie do przetwarzania danych jest uprawniona do ich przetwarzania w zakresie i czasie wskazanym w upoważnieniu.
7. Inspektor Ochrony Danych na podstawie wydanych upoważnień prowadzi ewidencję (rejestr zawierający imię i nazwisko oraz datę wydania upoważnienia) osób upoważnionych do przetwarzania danych.
8. Każda osoba upoważniana do przetwarzania danych osobowych składa pisemne oświadczenie o zachowaniu w tajemnicy przetwarzanych danych osobowych oraz znanych jej informacji o stosowanych wobec w/w danych środkach bezpieczeństwa.
9. Zatrudnieni, którzy w ramach swoich obowiązków przebywają w strefach gdzie przetwarzane są dane osobowe ale do ich obowiązków nie należy przetwarzanie danych osobowych muszą uzyskać przeszkolenie w zakresie ochrony danych osobowych i złożyć stosowne oświadczenie o przestrzeganiu zasad ochrony takich danych oraz o zachowaniu tajemnicy.

§ 7.

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe, do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięły w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać innym środkiem komunikacji elektronicznej.

§ 8.

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności, gdy informacje są kierowane do osoby małoletniej – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 niniejszej ustawy. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator jest obowiązany spełnić obowiązek informacyjny, wobec osoby, której dane uzyskano bezpośrednio po utrwaleniu zebranych danych.
3. Powyższy obowiązek Administrator nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonywania zgodnie z treścią dokumentów oraz klauzul informacyjnych. Przykładowe klauzule informacyjne stanowią załączniki do niniejszej Polityki, co nie zwalnia pracowników operujących na danych osobowych od zgłaszania Inspektorowi Ochrony Danych potrzeb w zakresie opracowania nowych klauzul.

REALIZACJA PRAW PRZEZ OSOBY, KTÓRYCH DANE DOTYCZĄ

§ 9

1. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa dostępu przysługującego osobie, której dane dotyczą należy:
   a) przedmiotowy wniosek przekazać do IOD, który przygotuje projekt odpowiedzi,
   b) odpowiedź na żądanie podpisuje Administrator lub osoba przez niego upoważniona,
   c) odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencję można również odesłać drogą elektroniczną,
   d) IOD prowadzi rejestr wpływających wniosków.
2. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do sprostowania danych należy:
   a) przedmiotowy wniosek przekazać do IOD,
   b) IOD zwraca się do ASI z prośbą o sprostowanie danych,
   c) c) ASI jest zobowiązany do sprostowania danych, o które wnioskował IOD w ciągu 10 dni,
   d) IOD przygotowuje projekt odpowiedzi na wniosek,
   e) odpowiedź na żądanie podpisuje Administrator lub osoba przez niego upoważniona,
   f) odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencję można wysłać również drogą elektroniczną,
   g) IOD prowadzi rejestr wpływających wniosków.
3. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do:
   a) usunięcia danych („prawo do bycia zapomnianym”),
   b) ograniczenia przetwarzania,
   c) przenoszenia danych,
   d) sprzeciwu,

   wniosek należy również przekazać do IOD.
4. Inspektor Ochrony Danych ocenia zasadność wniosku:
   a) w przypadku, gdy żądanie nie jest zasadne:
      - przygotowuje odpowiedź do akceptacji i podpisu Administratora lub osoby upoważnionej,
      - odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   b) w przypadku, gdy żądanie jest zasadne:
      - zwraca się do ASI z prośbą o realizację żądań zawartych we wniosku,

- ASI jest zobowiązany do realizacji wniosku IOD w ciągu 10 dni,
- IOD przygotowuje projekt odpowiedzi na wniosek,
- odpowiedź na wniosek podpisuje Administrator lub osoba upoważniona,
- odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,

c) IOD prowadzi rejestr opisanych powyżej wniosków.

5. ADO udziela odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki, najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania zobowiązany jest do podania przyczyny jej braku. Jeżeli żądanie ma skomplikowany charakter, a podmiot danych skierował dużą liczbę żądań, ADO może wydłużyć czas udzielenia odpowiedzi o kolejne dwa miesiące**,** jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu udzielenia odpowiedzi.
6. W przypadku jakichkolwiek zmian w zbiorach danych wynikających z realizacji praw osób, których dane dotyczą, ADO zobowiązany jest poinformować bez zbędnej zwłoki odbiorców, którym je udostępnił (przekazanie do wiadomości odpowiedzi kierowanej do adresata).

§ 10

1. Dane osobowe mogą być udostępniane w następujących przypadkach:
   - na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych na podstawie przepisów prawa,
   - na podstawie umowy powierzenia zawartej z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych osobowych.
2. Dane osobowe udostępnia się na pisemny umotywowany wniosek, chyba że istnieją przepisy stanowiące inaczej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§11.

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach i pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane, osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba, która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tę okoliczność IOD i Administratorowi.

4. Administrator i IOD podejmują wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

§ 12.

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach *(tzw. zasada „czystego biurka*).
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, który stał się nieużytecznym niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

§ 13.

1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, polegającego w szczególności na:
   - nieautoryzowanym dostępie do danych,
   - nieautoryzowanym modyfikowaniu lub zniszczeniem danych,
   - udostępnieniu danych nieautoryzowanym podmiotom,
   - nielegalnym ujawnieniem danych,
   - pozyskiwaniem danych z nielegalnych źródeł.
3. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych lub podejrzewa, że taka sytuacja miała miejsce, ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
4. W przypadku podejrzenia lub stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia

i udokumentowania zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub innych osób upoważnionych przez Administratora.

5. Wobec osoby, która naruszyła zasady ochrony danych osobowych lub w przypadku stwierdzonego naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby, zgodnie z określonymi zasadami wobec wymienionej osoby wszczyna się postępowanie dyscyplinarne, porządkowe lub karne. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby dokonującej naruszenia lub uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej z aktualnie obowiązującymi przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W przypadku podejrzenia lub stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić IOD i Administratora.
7. W przypadku opisanym w ust. 1 przeprowadza się sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.
8. Przy dokonywaniu sprawdzenia IOD oraz osobom wyznaczonym do współpracy z nim przez Administratora przysługują uprawnienia wskazane w rozporządzeniu ministra administracji i cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych, w szczególności prawo do:
   - utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
   - odebraniu wyjaśnień od osoby, której czynności objęto sprawdzeniem;
   - sporządzeniu kopii otrzymanego dokumentu;
   - sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych.
9. Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport (Załącznik nr 19).
10. Inspektor Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze, w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia przetwarzania danych osobowych oraz prowadzi Wykaz naruszeń według wzoru (Załącznik nr 17).
11. Jeżeli IOD jest długotrwale nieobecny Administrator w przypadku, o którym mowa w ust. 1 obowiązany jest przeprowadzić postępowanie wyjaśniające i ustalające skutki oraz przyczyny naruszenia lub narażenia na naruszenie zasad bezpieczeństwa

i sposobów zabezpieczenia, w sposób odpowiadający czynnościom podejmowanym przez IOD w przypadku sprawdzenia doraźnego.

POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 14

1. IOD podejmuje decyzje o wprowadzeniu zmian w środkach zabezpieczeń fizycznych oraz w systemie organizacji pracy, stosownie do mogących ponownie wystąpić naruszeń bezpieczeństwa danych osobowych.
2. ASI podejmuje decyzje odnośnie zmian w sposobie zabezpieczenia systemu informatycznego.
3. Administrator podejmuje decyzje o wyciągnięciu konsekwencji wobec osoby odpowiedzialnej za naruszenie zasad bezpieczeństwa.
4. IOD przekazuje do PUODO w terminie do 72 godzin, zgłoszenie (wg określonego wzoru w przepisach RODO), zawierające informacje o stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:
   - w przypadku przekroczenia 72 godzinnego terminu dodatkowo do zgłoszenia dołącza wyjaśnienia,
   - w przypadku gdy informacji nie może udzielić w tym samym czasie, udziela ją sukcesywnie bez zbędnej zwłoki.
5. IOD dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Poinformowanie bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. Należy przekazywać informację osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z PUODO, z poszanowaniem wskazówek przekazanych przez PUODO lub inne odpowiednie organy, takie jak organy ścigania. Zawiadomienie powinno przekazywać informację w jasnym i prostym języku a także zawierać:
   - opis charakteru naruszenia ochrony danych osobowych,
   - zalecenia dla danej osoby fizycznej, co do minimalizacji potencjalnych niekorzystnych skutków.
7. Poinformowanie, o którym mowa w pkt. 6 nie jest wymagane, jeśli PUODO stwierdzi, że spełniony został jeden z poniższych warunków:
   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c) w przypadku, kiedy wymagałoby ono niewspółmiernie dużego wysiłku - wydany zostanie publiczny komunikat lub zastosowany zostanie podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

§ 15.

Użytkownikowi systemu informatycznego zostaje nadany dostęp na podstawie „Karty zgłoszenia do systemu" (zmiany) do przetwarzania danych w systemie informatycznym, stanowiącej załącznik nr 18 do niniejszej Polityki, po uprzednim:

1. Zapoznaniu z przepisami dotyczącymi ochrony danych osobowych.
2. Podpisaniu oświadczenia o zapoznaniu się z niniejszą dokumentacją przetwarzania danych osobowych.
3. Podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych.
4. Otrzymaniu upoważnienia do przetwarzania danych osobowych.

POLITYKA HASEŁ

§ 16.

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora Systemu Informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemu informatycznego ADO jest obowiązany do:
   a) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających ich wykorzystanie do pracy w w/w systemie informatycznym;
   b) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   c) niezwłocznej zmiany hasła tymczasowego, przekazanego przez ASI;
   d) poinformowania ASI oraz IOD o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   e) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;

f) stosowania haseł nie posiadających w swojej strukturze części loginu;
g) stosowaniu haseł nie będących zbliżonymi do poprzednich (np.Tomasz$2013 - Tomasz$2014);
h) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.

5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
6. Zabronione jest:
   a) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   b) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   c) używaniu tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   d) udostępnianiu haseł innym użytkownikom;
   e) przeprowadzaniu prób łamania haseł;
   f) wpisywaniu haseł „na stałe" (np. w skryptach logowania) oraz wykorzystywaniu opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);
   g) po trzykrotnym, błędnym wprowadzeniu hasła użytkownik jest zobowiązany zgłosić ten fakt do Administratora Systemu Informatycznego, w celu zresetowania hasła dostępowego.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

§ 17.

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym tj. brak wykonywania jakichkolwiek czynności przez okres 5 minut w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć ich utraty.
5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:

a) wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
b) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§ 18.

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych podlega rejestrowaniu i może być monitorowana przez Administratora. Informacje przesyłane za pośrednictwem sieci Administratora (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika. Ponadto korespondencja służbowa realizowana drogą elektroniczną, zawierająca informacje wrażliwe winna zostać przesłana w formie zaszyfrowanej (zgodnie z instrukcją szyfrowania plików/katalogów przy pomocy narzędzia 7-Zip - załącznik nr 20) na adres mailowy wskazany przez stronę postępowania lub podmiot wykonujący prace zlecone na rzecz Starostwa Powiatowego w Czarnkowie. Dodatkowo w mailu lub przy użyciu innego komunikatora zostanie wskazany sposób odczytania przesłanych danych (z wykorzystaniem hasła).
4. Wszelka korespondencja elektroniczna prowadzona przez pracownika, a niezwiązana z działalnością Administratora, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Użytkownicy mają prawo korzystać z systemu poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
6. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych lub umownych, a także na wydajność systemu poczty elektronicznej.
7. Zabronione jest:
   a) wysyłanie bez zgody Administratora materiałów służbowych zawierających chronione dane na konta prywatne (np. celem pracy nad dokumentami poza miejscem pracy);
   b) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;

c) odbieranie przesyłek z nieznanych źródeł;
d) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
e) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych bez zgody Administratora;
f) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
g) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
h) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem (w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego);
i) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
j) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§ 19.

1. Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
2. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Dostęp użytkowników do sieci publiczne (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Wprowadza się całkowity zakaz w dostępie do treści niezgodnych z prawem lub niestosownych, a w szczególności pornograficznych, rasistowskich, traktujących o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§ 20.

Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do poniższych zasad:

1. Zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
2. Komputery przenośne należy przewozić jako bagaż podręczny;
3. Użytkownik wykonując czynności zawodowe lub umowne poza stałym miejscem wykonywania obowiązków powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
4. Zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
5. Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Starostwa Powiatowego w Czarnkowie;
6. W przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub administratora systemu informatycznego. Bezpośredni przełożony lub administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Inspektora Ochrony Danych, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;
7. Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi Systemu Informatycznego.

Zasady postępowania z nośnikami elektronicznymi oraz VPN w ramach tzw. pracy zdalnej zostaną określone odrębnym regulaminem pracy, wprowadzonym na czas jej trwania przez kierownika JO.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§ 21.

1. Do sprzętu komputerowego zalicza się między innymi komputery stacjonarne i przenośne, tablety, smartphony, drukarki, modemy, monitory, routery, osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.
2. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, Administrator Systemu Informatycznego informuje o powyższym Inspektora Ochrony Danych.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować, usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ

§ 22.

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji o danych osobowych lub informacji poufnych Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne Administratora, jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

§ 23.

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, oraz elektroniczne nośniki informacji.
2. Drogą przedostawania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
4. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z Administratorem Systemu Informatycznego.

POSTANOWIENIA KOŃCOWE

§ 24.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy z dnia 10 maja 2018 r.

o ochronie danych osobowych oraz 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).

3. Polityka jest dostępna w sieci Intranet Administratora Danych Osobowych.

Załączniki

1. Załącznik nr 1 – wzór zgody na przetwarzanie danych osobowych
2. Załącznik nr 2 – wzór upoważnienia do przetwarzanie danych osobowych,
3. Załącznik nr 3 – wzór upoważnienia do przebywania w obszarze przetwarzania
4. Załącznik nr 4 – wzór upoważnienia do odwołania upoważnienia i przebywania w obszarze przetwarzania danych osobowych
5. Załącznik nr 5 – Ogólna klauzula informacyjna,
6. Załącznik nr 6 - Klauzula informacyjna dot. przetwarzania danych osobowych w związku z ustawą z dnia29 sierpnia 1997 r. - Ordynacja podatkowa)
7. Załącznik nr 7 - Klauzula dot. debaty nad raportem o stanie powiatu - zgłoszenie chęci zabrania głosu
8. Załącznik nr 8 - Klauzula dot. debaty nad raportem o stanie powiatu – lista poparcia mieszkańców
9. Załącznik nr 9 - Klauzula informacyjna dot. skarg i wniosków
10. Załącznik nr 10 - Klauzula informacyjna dot. zdjęć/filmów upublicznianych przez Starostwo Powiatowe w Czarnkowie
11. Załącznik nr 11 - Klauzula informacyjna dot. Rzecznika Konsumentów
12. Załącznik nr 12 - Klauzula informacyjna Kandydaci do pracy
13. Załącznik nr 13 - Klauzula informacyjna Zatrudnieni
14. Załącznik nr 14 - Klauzula informacyjna Zamówienia publiczne i zaopatrzenie
15. Załącznik nr 15 - Klauzula informacyjna - o przetwarzaniu danych osobowych w celu realizacji zadań z zakresu ewidencji i oznaczania pojazdów,
16. Załącznik nr 16 - Klauzula informacyjna - o przetwarzaniu danych osobowych do wydawania zezwoleń, licencji i zaświadczeń związanych z transportem drogowym
17. Załącznik nr 17 – wzór wykazu incydentów powodujących naruszenie ochrony danych osobowych
18. Załącznik nr 18 -wzór karty zgłoszenia do systemu
19. Załącznik nr 19 – wzór raportu dot. naruszenia ochrony danych osobowych
20. Załącznik nr 20 - Instrukcja szyfrowania plików/katalogów przy pomocy narzędzia 7-Zip