Zarządzenie Nr 33/2018
Starosty Drawskiego
z dnia 23 lipca 2018 r.

w sprawie wprowadzenia zmian do „Polityki bezpieczeństwa Ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim" wprowadzonej Zarządzeniem nr 25/2018 Starosty Drawskiego z dnia 25 maja 2018 r.

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tekst jednolity Dz. U. z 2018 r., poz. 995 z późn. zm.) oraz art. 24 ust. 1 i 2 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)

zarządza się, co następuje:

§ 1

W „Polityce Bezpieczeństwa Ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim" stanowiącej Załącznik nr 1 do Zarządzenia nr 25/2018 Starosty Drawskiego z dnia 25 maja 2018 r. wprowadza się następujące zmiany:

1) w Spisie treści w pkt. 11 ZAŁĄCZNIKI:
   a) Nr 2 otrzymuje brzmienie: „Rejestr czynności przetwarzania";
   b) wykreśla się Nr 2a i 2b;
   c) Nr 16 otrzymuje brzmienie: „Regulamin Ochrony Danych Osobowych w Starostwie Powiatowym w Drawsku Pomorskim".
2) § 5 otrzymuje brzmienie: „Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy (w tym osoby fizyczne świadczące pracę w ramach umowy cywilnoprawnej) posiadający upoważnienie do przetwarzania danych osobowych. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Starostwie Powiatowym w Drawsku Pomorskim jest zobowiązana do zapoznania się z niniejszym dokumentem."
3) § 7 otrzymuje brzmienie: „Zgodnie z RODO, ADO prowadzi rejestr czynności przetwarzania danych osobowych. Wzór Rejestru czynności przetwarzania stanowi załącznik nr 2 do Polityki Bezpieczeństwa."
4) § 9 ust. 1 otrzymuje brzmienie: „Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni pracownicy Starostwa Powiatowego w Drawsku Pomorskim (w tym osoby fizyczne świadczące pracę w ramach umowy cywilnoprawnej) oraz pracownicy podmiotów świadczących usługi na jego rzecz w związku z realizacją jego określonych przepisami prawa celów i zadań (np. prace doraźne o charakterze serwisowym)."

Zatwierdzam pod względem formalnoprawnym

radca prawny Piotr Motyl

5) W § 13 ust. 1 lit. h dodaje się trzecie zdanie o treści: „Przed rozpoczęciem pracy klucze do pomieszczeń Wydziału Geodezji, Kartografii i Katastru są pobierane ze skrzynki znajdującej w pokoju nr 8 i tam też składowane po zakończeniu pracy."
6) § 17 ust. 4 otrzymuje brzmienie: „W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego należy pamiętać o następujących zasadach:
   - Nigdy nie wyjawiać nikomu swojej nazwy konta ani hasła.
   - Regularnie zmieniać hasło (minimum raz w miesiącu).

   Zespół Informatyków Starostwa Powiatowego przy użyciu automatycznych ustawień czuwa nad bezpieczeństwem systemu informatycznego poprzez:

   - Bieżącą aktualizację przeglądarek internetowych do najnowszej wersji.
   - Włączanie filtrów witryn wyłudzających informacje (phishing filter) w przeglądarce internetowej.
   - Regularne aktualizowanie systemu operacyjnego.
   - Regularne upewnianie się, że konta e-mail są poprawnie zabezpieczone.
   - Regularne upewnianie się, że komputery nie są zawirusowane."
7) § 20 ust. 2 otrzymuje brzmienie „Wzór wniosku o nadanie, pozbawienie, zmianę upoważnienia stanowi załącznik nr 11".
8) Załącznik nr 2 do Polityki bezpieczeństwa Ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim otrzymuje tytuł „Rejestr czynności przetwarzania";
9) usuwa się załączniki nr 2a i 2b do Polityki bezpieczeństwa Ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim;
10) Załącznik nr 16 do Polityki bezpieczeństwa Ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim otrzymuje tytuł „Regulamin Ochrony Danych Osobowych w Starostwie Powiatowym w Drawsku Pomorskim".

§ 2

Treść „Polityki bezpieczeństwa Ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim" uwzględniająca zmiany wprowadzone niniejszym dokumentem stanowi załącznik nr 1 do Zarządzenia.

§ 3

Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Stanisław Kuczyński

Sporządził: Magdalena Jaśniak

Załącznik nr 1
do Zarządzenia Starosty Drawskiego
Nr 33/2019 z dnia 23.07.2019 r.

POLITYKA BEZPIECZEŃSTWA

Ochrony danych osobowych
w Starostwie Powiatowym w Drawsku Pomorskim

SPIS TREŚCI

Zatwierdzam pod względem formalnoprawnym
radca prawny Piotr Motyl

Załącznik nr 1
do Zarządzenia Starosty Drawskiego
Nr 33 /2019 z dnia 23.01.2019 r.

ROZDZIAŁ I – POSTANOWIENIA OGÓLNE

§ 1

Celem Polityki Bezpieczeństwa ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim, dalej nazywanej *Polityką Bezpieczeństwa* (PB), jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania danych osobowych, a przede wszystkim zapewnienie ochrony przetwarzanych danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 2

Słownik pojęć stosowanych w niniejszej Polityce Bezpieczeństwa:

1) **Administrator Danych Osobowych (ADO)** – Starosta Drawski, decydujący o celach i sposobach przetwarzania danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim.
2) **Inspektor Ochrony Danych (IOD)** - osoba wyznaczona przez ADO do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych i prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych.
3) **Administrator systemu informatycznego (ASI)** - to osoba odpowiedzialna za nadzorowanie i utrzymanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony.
4) **RODO** – rozumie się przez to 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).
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) **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.
7) **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.

8) **Podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
9) **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.
10) **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.
11) **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.
12) **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.
13) **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14) **Użytkownik** – pracownik lub inna osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych.
15) **Nośnik** – każdy nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde itp.
16) **Sprzęt IT** – zespół urządzeń komputerowych służących do przetwarzania danych, w szczególności danych osobowych.

§ 3

1. Administratorem danych osobowych przetwarzanych w Starostwie Powiatowym w Drawsku Pomorskim jest Starosta Drawski.
2. Zakres danych osobowych przetwarzanych przez Użytkownika w Systemie nie może być szerszy niż powierzony do przetwarzania przez Administratora danych osobowych.
3. Dane osobowe przetwarzane w Systemie wykorzystywane są wyłącznie w celu realizacji określonych przepisami prawa celów i zadań Starostwa Powiatowego w Drawsku Pomorskim.

§ 4

Polityka Bezpieczeństwa określa:
a) granice dopuszczalnego zachowania Użytkowników Systemu stosowanego w Starostwie Powiatowym w Drawsku Pomorskim oraz wskazuje konsekwencje w stosunku do osób naruszających przepisy dotyczące ochrony danych osobowych,
b) prawa i obowiązki Użytkowników Systemu w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych w nim przetwarzanych,
c) sposób przetwarzania danych osobowych oraz środki organizacyjne

Zatwierdzam pod względem formalnoprawnym
radca prawny Piotr Motyl

i techniczne zapewniające ochronę tych danych,
d) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
e) wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych,
f) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych,
g) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
h) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
i) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
j) sposób przepływu informacji pomiędzy poszczególnymi systemami,
k) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych.

ROZDZIAŁ II – ZASADY PRZETWARZANIA DANYCH OSOBOWYCH. ODPOWIEDZIALNOŚĆ.

§ 5

Do stosowania zasad określonych przez dokumenty *Polityki Bezpieczeństwa* zobowiązani są wszyscy pracownicy (w tym osoby fizyczne świadczące pracę w ramach umowy cywilnoprawnej) posiadający upoważnienie do przetwarzania danych osobowych. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w Starostwie Powiatowym w Drawsku Pomorskim jest zobowiązana do zapoznania się z niniejszym dokumentem.

§ 6

1. Obszarem przetwarzania danych osobowych są:
    1. Budynki Starostwa Powiatowego w Drawsku Pomorskim:
        a. Plac Elizy Orzeszkowej 3, 78-500 Drawsko Pomorskie
        b. Plac Elizy Orzeszkowej 3a, 78-500 Drawsko Pomorskie
    2. Budynek Urzędu Miasta w Złocieńcu przy ul. Wolności 10 (parter, biuro nr 2 - Wydział Komunikacji i Transportu zamiejscowe stanowiska pracy w Złocieńcu)
2. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących **obszar przetwarzania** danych osobowych, stanowi *załącznik nr 1 do Polityki Bezpieczeństwa*.

§ 7

Zgodnie z RODO, ADO prowadzi rejestr czynności przetwarzania danych osobowych. Wzór Rejestru czynności przetwarzania stanowi załącznik nr 2 do *Polityki Bezpieczeństwa*.

§ 8

1. Wszystkie osoby, które przetwarzają dane osobowe w obszarze wymienionym w § 6, muszą posiadać pisemne **upoważnienie do przetwarzania danych** oraz podpisać **oświadczenie o zachowaniu poufności.**
2. Wzór upoważnienia, nadawanego przez ADO, stanowi *załącznik nr 3 do Polityki Bezpieczeństwa.* Wzór oświadczenia o zachowaniu poufności stanowi *załącznik nr 4 do Polityki Bezpieczeństwa.*

§ 9

1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni pracownicy Starostwa Powiatowego w Drawsku Pomorskim (w tym osoby fizyczne świadczące pracę w ramach umowy cywilnoprawnej) oraz pracownicy podmiotów świadczących usługi na jego rzecz w związku z realizacją jego określonych przepisami prawa celów i zadań (np. *prace doraźne o charakterze serwisowym).*
2. **Podmiot o którym mowa w ust. 1** zobowiązany jest do podpisania z ADO **umowy powierzenia przetwarzania danych osobowych**. Wzór umowy stanowi *załącznik nr 5* do Polityki Bezpieczeństwa.
3. Zakres danych osobowych powierzanych przez ADO powinien być **udokumentowany** w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi (*załącznik nr 6* do PB).

§ 10

1. Upoważnienia do przetwarzania danych osobowych w systemie informatycznym wydawane są zgodnie z właściwą procedurą określoną w niniejszym dokumencie oraz w *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w* Starostwie Powiatowym w Drawsku Pomorskim.
2. Upoważnienia, o których mowa w ust. 1 ważne są do dnia odwołania lub do chwili ustania zatrudnienia upoważnionego pracownika.

§ 11

Z uwzględnieniem wyjątków określonych w RODO, zabrania się przetwarzania danych 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.

§ 12

1. Na zasadach określonych w RODO dane osobowe mogą być wykorzystywane wyłącznie do celów do jakich były zbierane oraz powinny być przechowywane w formie uniemożliwiającej nieuprawnionym podmiotom identyfikację osób, których dotyczą.
2. W przypadku udostępniania dokumentów lub danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy dokonać anonimizacji tych danych.

Zatwierdzam pod względem formalnoprawnym
radca prawny Piotr Motyl

§ 13

W Starostwie Powiatowym w Drawsku Pomorskim stosuje się środki zabezpieczające zbiory danych w postaci **zabezpieczeń technicznych i organizacyjnych,** takich jak w szczególności:

1. Zabezpieczenia techniczne

a) Wejście do budynków Starostwa Powiatowego w Drawsku Pomorskim zabezpieczone jest zamkami drzwiowymi oraz alarmem.

b) Klucze do budynków posiada ochrona obiektów (otwieranie oraz zamykanie drzwi do budynków jak również uzbrajanie i rozbrajanie alarmu należy do ochrony), natomiast klucze zapasowe do budynków znajdują się w Wydziale Organizacyjnym. Klucze do pomieszczeń znajdują się w punkcie informacyjnym.

c) Klucze do pomieszczeń szczególnie chronionych - pomieszczenia Wydziału Zarządzania Kryzysowego, Kancelaria Tajna, pomieszczenie Zespołu Informatyków oraz Serwerownie pozostają pod osobistym nadzorem osób upoważnionych. Dostęp do tych pomieszczeń osób trzecich odbywa się pod ścisłym nadzorem.

d) Klucze do pomieszczeń wydziału komunikacji i transportu w Złocieńcu są zdawane do skrzynki w Urzędzie Miasta Złocieniec.

e) Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej i upoważnionej do przetwarzania danych lub w obecności Inspektora Ochrony Danych

f) Pomieszczenia, o których mowa wyżej, zamykane są na czas nieobecności pracownika w sposób uniemożliwiający dostęp do nich osobom trzecim. Pozostawienie kluczy w zamkach pomieszczeń, gdzie przetwarzane są dane osobowe jest niedopuszczalne (także podczas pobytu pracownika w pokoju).

g) W pomieszczeniach, w których przewiduje się przyjmowanie interesantów, monitory stanowisk komputerowych ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane.

h) Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy. Przed rozpoczęciem pracy klucze do pomieszczeń pobierane zostają z punktu informacyjnego i tam też składowane po zakończeniu pracy. Przed rozpoczęciem pracy klucze do pomieszczeń Wydziału Geodezji, Kartografii i Katastru są pobierane ze skrzynki znajdującej się w pokoju nr 8 i tam też składowane po zakończeniu pracy.

i) Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia zostaje zniszczony, w sposób uniemożliwiający jego odczytanie, przy pomocy niszczarki.

j) W pomieszczeniach, w których przewiduje się przyjmowanie interesantów w miejscu widocznym zamieszcza się klauzule informacyjne (których wzór stanowi załącznik nr 7 do PB).

2. Zabezpieczenia środków sprzętowych, informatycznych i telekomunikacyjnych:

a) urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej urządzeniem UPS,
b) dostęp fizyczny do sieci lokalnej jest ograniczony, centralny punkt dystrybucyjny sieci umieszczony jest w serwerowni - pokój nr 112,
c) dostęp do sieci WAN zabezpieczony jest firewall-em wraz z oprogramowaniem antywirusowym.

3. Zabezpieczenia organizacyjne:

a) Administrator danych wyznacza Inspektora Ochrony Danych, publikuje dane kontaktowe IOD oraz powiadamia o nich organ nadzorczy.
b) Zabezpieczenia ochrony fizycznej danych osobowych - Zabezpieczenia fizyczne opisane zostały w Załączniku nr 1 do PB.

4. Zabezpieczenia danych w wersji elektronicznej:

a) Dostęp do danych następuje po autoryzacji. Autoryzacja polega na podaniu identyfikatora oraz hasła. Uwzględniając kategorie przetwarzanych danych wprowadza się wysoki poziom bezpieczeństwa.
b) W przypadku, gdy zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego, minimalne wymagane zabezpieczenia obejmują: szyfrowanie dysku, po zakończeniu pracy przechowywanie komputera w warunkach zapewniających bezpieczeństwo danych, regularne wykonywanie kopii bezpieczeństwa.

5. Zabezpieczenia danych w rejestrach papierowych - dane przetwarzane w formie papierowej gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach itp. oraz przechowywane w zamykanych szafach.

§ 14

Odpowiedzialność

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością, w szczególności odpowiedzialnością karną.
2. Odpowiedzialności podlega każdy kto:
   - nie przestrzega przepisów o ochronie danych osobowych lub
   - nie przestrzega Polityki Bezpieczeństwa albo Instrukcji zarządzania systemem informatycznym.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z przepisów lub niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, co dotyczyć może w szczególności osoby, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie IOD.

Zatwierdzam pod względem formalnoprawnym
radca prawny Piotr Motyl

ROZDZIAŁ III – INSPEKTOR OCHRONY DANYCH

§ 15

1. Inspektor Ochrony Danych (IOD) to osoba wyznaczona przez Administratora Danych Osobowych, zobowiązana do:
   a) informowania administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub Rzeczpospolitej Polskiej o ochronie danych osobowych i doradzanie im w tej sprawie;
   b) monitorowania przestrzegania RODO i innych przepisów o ochronie danych osobowych oraz polityk ADO w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   d) współpracy z organem nadzorczym;
   e) pełnienia funkcji 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 konsultacji we wszelkich innych sprawach;
   f) prowadzenia wykazów, określonych w Załącznikach nr 1, 2, 2a, 2b, 6, 8 i 9 do PB;
   g) przeprowadzania **analizy ryzyk i zagrożeń** związanych z przetwarzaniem danych osobowych w systemie informatycznym;
   h) wykonywania innych zadań określonych w PB oraz zleconych przez ADO.
2. IOD jest również zobowiązany do podpisania oświadczenia o zachowaniu poufności (załącznik nr 4 do PB).

§ 16

IOD sygnalizuje Administratorowi Danych Osobowych potrzebę zmian w organizacji ochrony danych osobowych w Starostwie Powiatowym w Drawsku Pomorskim, w tym zmian w PB, oraz opracowuje projekty tych zmian.

ROZDZIAŁ IV - WARUNKI KORZYSTANIA Z SYSTEMU INFORMATYCZNEGO

§ 17

1. Zgodnie z postanowieniami niniejszej *Polityki bezpieczeństwa*, zabrania się Użytkownikowi systemu podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń systemu.
2. Każdy Użytkownik jest zobowiązany do zapoznania się i zaakceptowania zasad korzystania z systemu informatycznego, co potwierdza przez oświadczenie o zapoznaniu się z zasadami ochrony danych osobowych (Załącznik nr 10).
3. Oświadczenie, o którym mowa w ust. 2, jest warunkiem uzyskania dostępu do systemu.

4. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego należy pamiętać o następujących zasadach:
   - Nigdy nie wyjawiać nikomu swojej nazwy konta ani hasła.
   - Regularnie zmieniać hasło (minimum raz w miesiącu).

   Zespół Informatyków Starostwa Powiatowego przy użyciu automatycznych ustawień czuwa nad bezpieczeństwem systemu informatycznego poprzez:
   - Bieżącą aktualizację przeglądarek internetowych do najnowszej wersji.
   - Włączanie filtrów witryn wyłudzających informacje (phishing filter) w przeglądarce internetowej.
   - Regularne aktualizowanie systemu operacyjnego.
   - Regularne upewnianie się, że konta e-mail są poprawnie zabezpieczone.
   - Regularne upewnianie się, że komputery nie są zawirusowane.
5. **Bezwzględnie zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika**.
6. Zabronione jest udostępnianie innym osobom swoich haseł do systemów informatycznych kluczy albo kodów dostępu do pomieszczeń. Indywidualne hasło należy zachować jedynie dla siebie. Nie należy zamieszczać kartek z zapisanymi loginami i hasłami w miejscach widocznych. Nie należy przekazywać ich innym osobom, w tym przełożonemu lub administratorom, a jeśli już do tego doszło to powinno się je niezwłocznie zmienić.
7. Użytkownicy są zobowiązani do zachowania „zasady bezpiecznego ustawienia monitora", czyli ustawienia go w sposób uniemożliwiający osobom niepowołanym wgląd w przetwarzane dane. Przy wyjściu z pomieszczenia służbowego należy każdorazowo wcześniej zablokować dostęp do komputera.
8. Każdy pracownik zobowiązany jest do przestrzegania „zasady czystego biurka" poprzez:
   - przechowywanie na biurku dokumentów zawierających informacje podlegające ochronie w taki sposób, aby dostępu do tych dokumentów nie miały osoby nieuprawnione,
   - po zakończeniu pracy umieszczanie nośników informacji w szafie lub szufladzie, zamykając je na klucz, a jeśli pracownik wychodzi jako ostatni, to upewnianie się, że zostawia pomieszczenie zamknięte na klucz.
9. Użytkownik jest zobowiązany do przestrzegania „zasady czystej drukarki/kopiarki/skanera": drukowane, kopiowane czy skanowane informacje powinny być zabierane z drukarek/kserokopiarek/skanerów niezwłocznie po wydrukowaniu/skopiowaniu/zeskanowaniu. W przypadku nieudanej próby wydrukowania/skopiowania/zeskanowania użytkownik powinien skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru.
10. Użytkownik jest zobowiązany do przestrzegania „zasady czystego kosza". W przypadku pracy na dokumentach w formie papierowej, należy pamiętać, że dokumenty papierowe, z wyjątkiem materiałów jawnych (np. promocyjnych, marketingowych oraz informacyjnych) powinny być niszczone w sposób uniemożliwiający ich ponowne odczytanie np. w niszczarce. Nie wolno wyrzucać do kosza na śmieci żadnych dokumentów lub nośników zawierających informacje podlegające ochronie.

Zatwierdzam pod względem formalnoprawnym
radca prawny Piotr Motyl

11. Dokumenty zawierające informacje chronione, podlegające usunięciu należy zniszczyć w taki sposób, aby nie dało się odtworzyć ich treści (zwłaszcza zidentyfikować osób, których dane się tam pojawiają). Nie należy zostawiać takich dokumentów na biurku umożliwiając dostęp do nich osobom nieuprawnionym.
12. Po zakończeniu pracy należy wylogować się z wszystkich służbowych systemów.

§ 18

1. Do prawidłowego korzystania z systemu informatycznego niezbędne są:
   a) połączenie z siecią Internet;
   b) zainstalowana przeglądarka internetowa: Mozilla Firefox, Google Chrome lub Internet Explorer w najnowszej, stabilnej wersji;
   c) zainstalowana przeglądarka plików w formacie PDF.
2. przeglądarkę internetową należy skonfigurować tak, aby miała włączoną obsługę protokołu OCSP (Online Certificate Status Protocol), umożliwiającego przeprowadzenie weryfikacji ważności certyfikatu.

§ 19

1. Należy przestrzegać następujących zasad bezpiecznych haseł:
   - hasła składają się co najmniej z 8 znaków,
   - hasła składają się z dużych i małych liter oraz z cyfr lub znaków specjalnych
   - wymagana jest okresowa zmiana hasła,
   - nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów,
   - użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności,
   - zabronione jest zapisywanie haseł w sposób jawny, przekazywanie ich innym osobom lub umożliwianie dostępu do nich innym osobom.
2. Czas trwania nieaktywnej sesji (czas bezczynności) po jakim następuje automatyczne wylogowanie Użytkownika wynosić powinien maksymalnie 10 minut (co nie zwalnia pracownika z obowiązku każdorazowego wylogowania się z systemu).
3. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie dokonać zmiany hasła na nowe.
4. W przypadku braku możliwości samodzielnego dokonania przez Użytkownika zmiany hasła, należy powiadomić ASI.

§ 20

Procedura nadawania/zmiany/odwołania upoważnień do przetwarzania danych w systemie informatycznym:

1. Bezpośredni przełożony pracownika kieruje do Inspektora ochrony danych wniosek o nadanie upoważnienia do przetwarzania danych osobowych określając:
   a) niezbędne dane użytkownika,
   b) zbiór danych osobowych,
   c) zakres systemów informatycznych.

2. Wzór wniosku o nadanie, pozbawienie, zmianę upoważnienia stanowi załącznik nr 11.
3. IOD przekłada wniosek Administratorowi Danych Osobowych do akceptacji.
4. Po zaakceptowaniu wniosku przez ADO, Administrator Systemów Informatycznych nadaje uprawnienia dostępu do zasobów (login i hasło umożliwiające dostęp do wszystkich systemów i aplikacji w zakresie określonym we wniosku i zaakceptowanym przez ADO).
5. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3.
6. Modyfikacja lub odebranie pracownikowi uprawnień w systemie informatycznym następuje na pisemny wniosek przełożonego pracownika i podlega procedurze takiej samej jak przy nadawaniu uprawnień.
7. Identyfikator osoby, która utraciła upoważnienie do przetwarzania danych osobowych lub uprawnienia dostępu do systemu informatycznego należy niezwłocznie zablokować i nie należy go nadawać innym użytkownikom.

ROZDZIAŁ V – ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY

§ 21

Stosuje się następujące procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla Użytkowników systemu informatycznego.

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do powiadomienia ASI i IOD o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu w dane wyświetlane na monitorach komputerowych, na których pracuje.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki, na których znajdują się dane osobowe,
   c) upewnić się czy komputer został wyłączony.

ROZDZIAŁ VI - POCZTA ELEKTRONICZNA, INTERNET W SYSTEMIE

§ 22

1. W systemie informatycznym wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w systemie.
2. Użytkownik zobowiązany jest do dbania o bezpieczeństwo konta mailowego, o którym mowa powyżej, w szczególności do:
   a) używania silnego hasła dostępu;

Zatwierdzam pod względem formalnoprawnym
radca prawny Piotr Motyl

b) nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł;
c) zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej lub wydającej się pochodzić od znanych nadawców.

3. Użytkownik zobowiązany jest do korzystania z sieci Internet w sposób, który nie zagraża bezpieczeństwu danych gromadzonych i przetwarzanych w systemie.

ROZDZIAŁ VII – POSTĘPOWANIE NA WYPADEK ZAGROŻENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 23

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) próby naruszenia ochrony danych:

      - z zewnątrz – np. włamania do systemu, podsłuch, kradzież danych
      - z wewnątrz – np. nieumyślna lub celowa modyfikacja danych, kradzież danych

   b) programy destrukcyjne, np. wirusy, konie trojańskie, makra, bomby logiczne,
   c) awarie sprzętu lub uszkodzenie oprogramowania,
   d) zabór sprzętu lub nośników z ważnymi danymi,
   e) usiłowanie zakłócenia działania systemu informatycznego,
   f) inne zdarzenia skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.
2. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń lub dokumentów,
   b) niewłaściwe zabezpieczenie sprzętu IT lub oprogramowania przed wyciekiem, kradzieżą albo utratą danych osobowych,
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
   d) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   e) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   f) 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).
3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:
   a) zgłoszenia od Użytkowników,
   b) alarmy z systemów informatycznych,
   c) analizy incydentów,

d) wyniki audytów / kontroli.

§ 24

Każdy pracownik Starostwa Powiatowego w Drawsku Pomorskim, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest niezwłocznie poinformować o nich Inspektora Ochrony Danych.

§ 25

W przypadku stwierdzenia **wystąpienia zagrożenia**, Inspektor Ochrony Danych 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 postępowanie.

§ 26

Inspektor Ochrony Danych jest odpowiedzialny za **analizę incydentów bezpieczeństwa, zagrożeń lub słabości systemu** ochrony danych osobowych. W przypadku **stwierdzenia incydentu** (naruszenia ochrony danych osobowych) IOD prowadzi postępowanie wyjaśniające, w toku którego:

a) ustala czas wystąpienia incydentu, jego źródło, zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
b) zabezpiecza ewentualne dowody, ustala osoby odpowiedzialne za naruszenie,
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 w rejestrze incydentów (załącznik nr 12),
h) sporządza protokół z wystąpienia incydentu (załącznik nr 13),
i) niezwłocznie oraz w terminie wskazanym w RODO zgłasza w imieniu ADO incydent organowi nadzorczemu, a w przypadku przekroczenia terminu dołącza wyjaśnienie przyczyn opóźnienia,
j) na zasadach określonych w RODO, zawiadamia w imieniu ADO osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

§ 27

Inspektor Ochrony Danych jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

Zatwierdzam pod względem formalnoprawnym
radca prawny Piotr Motyl

ROZDZIAŁ VIII – KONTROLA SYSTEMU OCHRONY DANYCH OSOBOWYCH

§ 28

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z kontrolą stanu bezpieczeństwa danych osobowych.
2. Procedura obejmuje wszystkie Wydziały Starostwa Powiatowego w Drawsku Pomorskim.
3. Do kontroli stanu ochrony danych osobowych upoważniony jest IOD.
4. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami prawa ochrony danych osobowych i PB.
5. Inspektor ochrony danych przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.
6. Kontrola przeprowadzana jest na podstawie listy kontrolnej (Załącznik nr 14).
7. Po dokonanej kontroli IOD przygotowuje i przekazuje raport pokontrolny (Załącznik nr 15) Naczelnikowi kontrolowanego wydziału oraz Administratorowi Danych Osobowych. Na jego podstawie IOD inicjuje działania korygujące lub zapobiegawcze.
8. Raz w roku Inspektor Ochrony Danych przygotowuje sprawozdanie roczne ze stanu funkcjonowania systemu ochrony danych osobowych.
9. Sprawozdanie przygotowane przez IOD sporządzane jest na podstawie raportów pokontrolnych wydziałów kontrolowanych, a następnie przedstawiany jest Administratorowi Danych Osobowych.

ROZDZIAŁ IX – SZKOLENIA

§ 29

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych oraz zapoznać się z Regulaminem Ochrony Danych Osobowych w Starostwie Powiatowym w Drawsku Pomorskim (Załącznik nr 16).
2. Za przeprowadzenie szkolenia odpowiada IOD a za jego zorganizowanie odpowiada przełożony użytkowników.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ochrony danych osobowych oraz instrukcjami obowiązującymi u Administratora Danych, a także zobowiązania się do ich przestrzegania. Harmonogram szkolenia wraz z listą obecności określono w Załączniku nr 17.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza potwierdzenia obecności oraz zobowiązania do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
5. Dokument (Załącznik nr 10 - Oświadczenie) jest przechowywany przez IOD i stanowi podstawę do podejmowania działań w celu nadania użytkownikom uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

ROZDZIAŁ X – POSTANOWIENIA KOŃCOWE

§ 30

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ochrony danych osobowych, w szczególności RODO i krajowych aktów wdrażających i doprecyzowujących jego postanowienia.

§ 31

Niniejszy dokument wchodzi w życie z dniem 25 maja 2018 r.

STAROSTA

Stanisław Kuczyński

podpis Administratora Danych Osobowych

Zatwierdzam pod względem formalnoprawnym

radca prawny Piotr Motyl