ZARZĄDZENIE NR 133 / 2017
STAROSTY PUCKIEGO
z dnia 27 grudnia 2017 r.

w sprawie: wprowadzenia „Polityki Bezpieczeństwa Danych Osobowych w Starostwie Powiatowym w Pucku"

Na podstawie: art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.) oraz § 38 ust. 1 Regulaminu Organizacyjnego Starostwa Powiatowego w Pucku zarządza się, co następuje:

§ 1

Wprowadzam „Politykę Bezpieczeństwa Danych Osobowych w Starostwie Powiatowym w Pucku", stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Traci moc obowiązującą zarządzenie nr 37/2009 z dnia 1 października 2009 r. w sprawie wprowadzenia „Polityki Bezpieczeństwa Ochrony Danych Osobowych w Starostwie Powiatowym w Pucku".

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Jarosław Białk

Załącznik
do zarządzenia nr 133/2017
z dnia 27 grudnia 2017r.

Polityka Bezpieczeństwa Danych Osobowych

w Starostwie Powiatowym w Pucku

Zatwierdził:	Data:
STAROSTA Jarosław Białk	27.12.2017r.

I. Wstęp

1. Polityka Bezpieczeństwa Danych Osobowych w Starostwie Powiatowym w Pucku, zwana dalej „Polityką" została opracowana zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

II. Obowiązki Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji

2. Administratorem Danych Osobowych (ADO) jest Starosta Pucki.
3. ADO deklaruje gotowość budowy kompleksowego systemu zarządzania bezpieczeństwem informacji oraz wsparcie wszelkich działań mających na celu ochronę zasobów informacyjnych Starostwa.
4. ADO może powołać Administratora Bezpieczeństwa Informacji (ABI) a w razie jego niepowołania ADO realizuje zadania ABI.
5. Do najważniejszych obowiązków ABI należy:
   1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO,
   2) przestrzeganie zasad określonych w dokumentacji, o której mowa w art. 36 ustawy,
   3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
   4) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów zawierających dane wrażliwe,
   5) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
   6) zapewnienie przetwarzania danych zgodnie z uregulowaniami polityki bezpieczeństwa informacji,
   7) wydawanie i cofanie upoważnień do przetwarzania danych osobowych,
   8) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   9) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
   10) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
6. ABI ma prawo:
   1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Starostwie,
   2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,

3) żądania od pracowników pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

III. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

7. ABI prowadzi wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.
8. Wzór wykazu stanowi załącznik nr 1 do Polityki.

IV. Zbiory danych osobowych

9. ABI prowadzi wykaz zbiorów danych osobowych (w tym zbiorów powierzonych do przetwarzania) i programów użytych do przetwarzania tych danych.
10. Wzór wykazu stanowi załącznik nr 2 do Polityki.

V. Struktura zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

11. ABI opracowuje i na bieżąco aktualizuje:
    1) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
    2) sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe.

VI. Uprawnienia do przetwarzania danych osobowych.

12. Przyznanie, anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym wraz z uprawnieniami do przetwarzania tych danych wymaga pisemnego upoważnienia udzielonego przez ABI według wzoru stanowiącego załącznik nr 3 do Polityki. O udzieleniu upoważnienia informowany jest ASI celem nadania identyfikatora oraz uprawnień użytkownika w systemach informatycznych i aplikacjach.
13. Przed nadaniem upoważnienia, ABI zobowiązany jest do sprawdzenia, czy osoba upoważniona:
    1) odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z Polityką,
    2) podpisała oświadczenie o zachowaniu poufności,
    3) będzie przetwarzać dane osobowe w zakresie i celu określonym upoważnieniu.

14. Jeśli jest to wymagane, przełożony określa dla osoby upoważnionej jej zakres uprawnień w systemach informatycznych.
15. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login).
16. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
17. ABI odpowiada za przechowywanie i aktualizację wszystkich upoważnień
18. ABI opowiada za prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji określa załącznik nr 4 do Polityki).

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

19. Zabezpieczenia organizacyjne:
    1) została opracowana i wdrożona niniejsza Polityka praz instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe,
    2) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,
    3) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
    4) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
    5) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy,
    6) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
    7) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
20. Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej:
    1) drzwi do pomieszczeń zamykane na klucz,
    2) zamykane na klucz niemetalowe lub metalowe szafy
    3) niszczarki dokumentów
    4) system alarmowy przeciwwłamaniowy.
21. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
    1) zastosowano UPS do serwera lub kluczowych komputerów, na których są przetwarzane dane osobowe,
    2) dostęp do komputera zawierającego dane osobowe odbywa się poprzez podanie loginu i hasła,
    3) w przypadku dostępu do danych osobowych przez Internet, stosuje się szyfrowanie tego połączenia (SSL lub VPN),
    4) w przypadku dostępu do danych osobowych przez Internet, należy uprzednio podać login i hasło,
    5) zastosowano system antywirusowy,

6) użyto system Firewall do ochrony dostępu do sieci komputerowej,
7) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej,
8) użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

22. Zabezpieczenia programów przetwarzających dane osobowe:
1) dla osób upoważnionych do przetwarzania danych osobowych określono zakres przetwarzania (zakres obowiązków),
2) dostęp do danych osobowych w systemach informatycznych wymaga podania nazwy użytkownika oraz hasła,
3) użytkownicy systemów informatycznych posiadają w nich konta z określonymi uprawnieniami,
4) zastosowano zahasłowane wygaszacze ekranu uruchamiane po dłuższej nieaktywności użytkownika,
5) zmianę haseł wymusza system,
6) dane osobowe są zaszyfrowane na twardych dyskach lub w bazach danych,
7) systemy informatyczne pozwalają na rejestrację kluczowych operacji użytkowników wykonywanych na danych osobowych.

VIII. Odpowiedzialność osób przetwarzających dane

23. Osoby przetwarzające dane osobowe zobowiązane są w szczególności do:
1) bieżącego nadzoru nad dokumentacją zawierającą dane osobowe,
2) niepozostawiania bez kontroli dokumentów w miejscach publicznych oraz w samochodach,
3) nieużywania powtórnie dokumentów zadrukowanych jednostronnie,
4) opuszczania stanowiska pracy dopiero po zabezpieczeniu dokumentów,
5) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej,
6) niszczenia w niszczarce nieprzydatnych dokumentów zawierających dane osobowe przed opuszczeniem miejsca pracy,
7) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych,
8) zachowania w tajemnicy danych, w tym także wobec najbliższych,
9) zamykania po zakończeniu dnia pracy,
10) zamykania drzwi na klucz po zakończeniu pracy.

IX. Postępowanie w przypadku naruszenia zasad ochrony danych osobowych

24. Naruszeniem zasad ochrony danych osobowych w rozumieniu Polityki (dalej jako „incydent") jest każde zdarzenie, zależne jak i niezależne od woli ludzkiej, powodujące zagrożenie bezpieczeństwa danych osobowych, w szczególności:
1) prowadzące do utraty integralności danych (np. pozostawianie dokumentów zawierających dane w miejscach powszechnie dostępnych),
2) zagrażające poufności danych (np. przesyłanie danych drogą elektroniczną bez zabezpieczenia dostępu do plików),

3) zagrażające rozliczalności danych (np. korzystanie przez kilka osób z jednego hasła dostępu).

25. W razie stwierdzenia lub podejrzenia wystąpienia incydentu należy niezwłocznie:
    1) wysłuchać relacji zawiadamiającego, jak również każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem, w celu oceny zaistniałej sytuacji,
    2) poinformować o zaistniałym zdarzeniu ABI lub ADO,
    3) utrwalić wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności:
        a) dokładny czas uzyskania informacji stwierdzającej albo uzasadniającej podejrzenie naruszenia ochrony danych osobowych albo samodzielnego wykrycia tego faktu,
        b) dane osoby zgłaszającej,
        c) stan zabezpieczeń,
    4) podjąć niezwłocznie wszelkie działania zmierzające do odzyskania utraconych danych albo zabezpieczenia danych przed utratą,
    5) podjąć niezwłocznie wszelkie działania zmierzające do ustalenia przyczyn zdarzenia, jak i okoliczności sprzyjających naruszeniu,
    6) podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych.
26. ABI niezwłocznie od momentu ustalenia przyczyn oraz okoliczności sprzyjających naruszeniu, nie później jednak niż w terminie 14 dni od naruszenia, winien sporządzić raport o przyczynach, przebiegu i wnioskach z incydentu.
27. W raporcie winny znaleźć się informacje o:
    1) dacie i godzinie powiadomienia,
    2) dacie i godzinie naruszenia,
    3) środkach podjętych przez zawiadamiającego,
    4) podjętych działaniach wraz z ich uzasadnieniem,
    5) analizie przyczyn oraz okoliczności sprzyjających naruszeniu.

Wykaz załączników do Polityki:

1) Wzór wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
2) Wzór wykazu zbiorów danych osobowych
3) Wzór upoważnienia do przetwarzania danych osobowych
4) Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Zał. nr 1 do Polityki

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Lp.	Adres budynku	Numer pokoju	Komórka organizacyjna użytkująca pomieszczenie	Rodzaj zastosowanego zabezpieczenia

.....
data i podpis ABI

Zał. nr 2 do Polityki

Wykaz zbiorów danych osobowych

Lp.	Nazwa zbioru danych	Program służący do przetwarzania baz danych lub nazwa zbioru papierowego	Lokalizacja	Zabezpieczenia fizyczne

.....
data i podpis ABI

Załącznik nr 3 do Polityki

Egz. nr ...

Puck, dnia .....

U P O W A Ż N I E N I E N R .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922)

upoważniam:

Panią/Pana .....

do przetwarzania danych osobowych znajdujących się w zbiorach i ewidencjach prowadzonych przez Starostwo Powiatowe w Pucku w zakresie w jakim jest to niezbędne do wykonywania obowiązków służbowych. Upoważnienie to obejmuje również uprawnienie do przetwarzania danych osobowych w systemie informatycznym Starostwa Powiatowego w Pucku.

Upoważnienie niniejsze zostaje udzielone na czas nieoznaczony z tym, że wygasa ono z chwilą wcześniejszego ustania stosunku pracy Pani/Pana..... w Starostwie Powiatowym w Pucku.

Załącznik nr 4 do Polityki

Ewidencja upoważnień do przetwarzania danych osobowych

L.p.	Nazwisko	Imię	Stanowisko służbowe	Data udzielenia	Czas na jaki zostało udzielone	Zakres udzielonego upoważnienia lub pełnomocnictwa	Numer
1							
2							
3							
4							
5							
6							
7							
8							
9							