ZARZĄDZENIE NR 18/2016

STAROSTY ŁOWICKIEGO

z dnia 21 marca 2016 r.

w sprawie wprowadzenia *Regulaminu ochrony danych osobowych w Starostwie Powiatowym w Łowiczu.*

Na podstawie art. 34 ust. 1 i art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (t.j. Dz. U. z 2015 r. poz. 1445,1890) oraz Zarządzenia Nr 17/2016 Starosty Łowickiego z dnia 21 marca 2016 r. w sprawie wprowadzenia dokumentacji zapewniającej ochronę przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu wraz z opisem środków technicznych i organizacyjnych stosowanych w jednostce zarządzam, co następuje:

§1. Wprowadzam *Regulamin ochrony danych osobowych w Starostwie Powiatowym w Łowiczu*, stanowiący załącznik do niniejszego zarządzenia.

§2. Nadzór nad wykonaniem zarządzenia powierzam Sekretarzowi Powiatu Łowickiego.

§3. Zarządzenie wchodzi w życie z dniem 04 kwietnia 2016 r.

STAROSTA ŁOWICKI

Krzysztof Figat

Uzasadnienie:

Celem opracowania i wdrożenia *Regulaminu* jest poszerzenie wiedzy i świadomości pracowników dotyczącej bezpieczeństwa przetwarzania danych osobowych i zagadnień z tym związanych.
Regulamin ochrony danych osobowych Starostwa Powiatowego Łowiczu opisuje jak bezpiecznie, z zachowaniem wszystkich procedur zawartych w polityce bezpieczeństwa w pracy codziennej, wykonywanej przez pracowników i współpracowników Starostwa, przetwarzać dane osobowe.
Regulamin jest jawny i udostępniany pracownikom w sposób powszechnie przyjęty przez Administratora dla wewnętrznych aktów normatywnych.

Załącznik
do Zarządzenia Nr 18/20016
Starosty Łowickiego
z dnia 21 marca 2016 roku

REGULAMIN
OCHRONY DANYCH OSOBOWYCH
w
Starostwie Powiatowym w Łowiczu

Dokument do użytku wewnętrznego

Marzec 2016

SPIS TREŚCI

DEFINICJE

Ilekroć w niniejszym regulaminie jest mowa o:

1) **Administratorze danych** rozumie się przez to Starostę Łowickiego, który decyduje o celach i środkach przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu, dalej zwanego „Administratorem";

2) **Administratorze bezpieczeństwa informacji** – rozumie się przez to osobę wyznaczoną przez Administratora, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami ustawy i rozporządzenia, zwaną dalej „ABI";

3) **Administratorze systemów informatycznych** – 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 ustawą i rozporządzeniem, zwaną dalej „ASI";

4) **Kierowniku** – rozumie się przez to bezpośredniego przełożonego osób zatrudnionych w biurze/wydziale/samodzielnym stanowisku w Starostwie Powiatowym w Łowiczu.

5) **Danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zwane dalej „dane";

6) **Osobie upoważnionej** – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;

7) **Użytkowniku systemu** – rozumie się przez to osobę upoważnioną, posiadającą dostęp do sieci LAN umożliwiający korzystanie z sieci Internet oraz login i hasło do systemu;

8) **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;

9) **Upoważnieniu** – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;

10) **Ustawie** – rozumie się przez to ustawę z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2015 r. poz. 2135);

11) **Rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz.U. Nr 100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

12) **Zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE

§1.1 W celu zapewnienia ochrony przetwarzanych danych osobowych zarówno za pomocą systemów informatycznych jak i w wersji papierowej Administrator wdrożył politykę

bezpieczeństwa przetwarzania danych osobowych oraz instrukcję zarządzania systemem informatycznym do przetwarzania danych osobowych.

2.Każdy z pracowników/współpracowników ma obowiązek zapoznać się z zasadami ochrony danych osobowych opisanymi w niniejszym regulaminie, na który składają się postanowienia zawarte w polityce bezpieczeństwa oraz instrukcji zarządzania, przydatne dla każdej osoby przetwarzającej dane podczas codziennego wykonywania obowiązków zawodowych.

3. Celem Regulaminu jest zapewnienie bezpieczeństwa procesu przetwarzania danych osobowych poprzez identyfikację potencjalnych zagrożeń oraz opracowanie, wdrożenie i stałe monitorowanie funkcjonowania mechanizmów i uregulowań umożliwiających minimalizację i eliminację tych zagrożeń.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW INFORMATYCZNYCH

§2.1. Administrator wyznacza odrębnym zarządzeniem i zgłasza do rejestru prowadzonego przez GIODO administratora bezpieczeństwa informacji, który jest odpowiedzialny za przetwarzanie danych zgodnie z ustawą oraz rozporządzeniem.

2. Zgodnie z przyjętą polityką delegowania uprawnień i zastępowalności Administrator wyznacza zastępcę ABI, osoba taka spełnia warunki z rozporządzenia jak dla ABI.

3. Zastępcą ABI jest ASI, który wykonuje wszystkie obowiązki należące do zakresu obowiązków ABI podczas jego nieobecności.

§3.1. Administrator wyznacza odrębnym zarządzeniem administratora systemów informatycznych.

2. Zgodnie z przyjętą polityką w Starostwie Powiatowym w Łowiczu w zakresie delegowania uprawnień i zastępowalności Administrator wyznacza zastępcę ASI.

3. Zastępca ASI wykonuje wszystkie obowiązki należące do zakresu obowiązków ASI podczas jego nieobecności.

§4.1. W przypadku powzięcia jakichkolwiek wątpliwości, co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do ABI z wnioskiem (ustnie/pisemnie) o ich rozstrzygnięcie.

2. Przed udzieleniem przez ABI 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

§5.1. Administrator, na pisemny wniosek kierownika, nadaje upoważnienie do przetwarzania danych osobowych każdej osobie, która do przetwarzania danych będzie dopuszczona. Wydanie upoważnienia jest związane z podpisaniem przez upoważnionego stosownego oświadczenia, potwierdzającego znajomość przepisów w tym zakresie.

Wzór wniosku, stanowi załącznik nr 4 ***Wniosek o nadanie uprawnień*** do polityki bezpieczeństwa.

2. Upoważnienie zawiera:
   1) datę z którą zostało nadane, znak sprawy(z rejestru upoważnień);
   2) datę z którą upoważnienie wygasa, jeżeli jest ono nadane na czas określony;
   3) zakres upoważnienia.

3. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.

4. Zmiana stanowiska lub/i inny zakres obowiązków jest związany z koniecznością złożenia przez kierownika wniosku do Administratora o nadanie nowego upoważnienia i cofnięcia poprzednich.

5. Na podstawie złożonego wniosku, o którym mowa w ust.1, po zaakceptowaniu przez ABI są przygotowywane dokumenty. Wniosek można przekazać w wersji papierowej lub elektronicznie na adres e-mail ABI.

6. Upoważnienie wraz z oświadczeniem jest przygotowywane w trzech egzemplarzach. Podpisane przez Administratora upoważnienie ABI przekazuje kierownikowi. Pracownik po zapoznaniu się z przepisami z zakresu ochrony danych osobowych i odbytym szkoleniu, o którym mowa w ust.10 potwierdza, składając podpis, znajomość przepisów w tym zakresie.
Kierownik przekazuje podpisane trzy egzemplarze, jeden pracownikowi, dwa wydziałowi organizacyjnemu oraz niezwłocznie drogą elektroniczną informuje ABI o tym fakcie, podając datę przyjęcia upoważnienia przez osobę upoważnioną.
Wzór upoważnienia stanowi załącznik nr 5 ***Upoważnienie do przetwarzania danych osobowych,*** natomiast wzór oświadczenia stanowi załącznik nr 6 ***Oświadczenie*** do polityki bezpieczeństwa.

7. Odpowiedzialność służbową za przetwarzanie danych osobowych tylko przez osoby, które przeszły szkolenie i są upoważnione przez Administratora danych osobowych, ponosi kierownik. Skierowanie na szkolenie, termin kierownik ustala wysyłając zgłoszenie pocztą elektroniczną do ABI.

8. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.

9. Zachowanie tajemnicy w zakresie danych osobowych dotyczy również wszystkich osób wykonujących zadania na rzecz Starostwa oraz pełniących funkcję w administracji budynków do których mają dostęp, zarówno zamierzony jak i przypadkowy, do wszelkich informacji, które powzięły w czasie pracy w Starostwie Powiatowym w Łowiczu. Obowiązek zachowania danych w tajemnicy jest bezterminowy, udokumentowany podpisanym oświadczeniem, które jest załączone do akt osobowych/ umowy.
Wzór oświadczenia stanowi załącznik nr 6a ***Oświadczenie*** do polityki bezpieczeństwa.

10. Szkolenie dla osób, które mają otrzymać upoważnienie w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych jest prowadzone przez ABI/inne podmioty. W szkoleniu uczestniczą również osoby, od których należy odebrać oświadczenie, o którym mowa w ust.9.

11. Szkolenie **wstępne** jest przeprowadzane przed dopuszczeniem osoby upoważnionej do czynności przetwarzania danych, przed nadaniem upoważnienia lub odebrania oświadczenia o zachowaniu tajemnicy.

12. Szkolenia **cykliczne**, minimum raz w roku dla wszystkich pracowników oraz zarządu prowadzi ABI lub/i ASI. Z przeprowadzonego szkolenia jest sporządzana lista obecności. Wiedza z zakresu ochrony danych osobowych jest systematycznie sprawdzana. ABI informuje kierowników o terminach i formie sprawdzenia wiedzy. Wyniki są przekazywane w formie pisemnej do Administratora, celem podjęcia stosownych działań.

§ 6.1. 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. Wszyscy pracownicy są zobowiązani do bezwzględnego umieszczenia w swoich e-mailach służbowych informacji identyfikującej pracownika wraz z podaniem stanowiska, wydziału/ biura, telefonu służbowego oraz umieszczenia w stopce informacji (wg. wzoru):

w podpisie

Aneta Kowalska
Inspektor w Wydziale Komunikacji
Starostwo Powiatowe w Łowiczu
ul. Stanisławskiego 28 99-400 Łowicz
Tel:
e-mail;

w stopce

Powiat Łowicki 99-40 Łowicz ul. Stanisławskiego 30
tel.: +48 46 837-59-02; fax. +48 46 837 50 15; NIP: 834-18-82-519; Regon: 750 14 77 68,
Treść tej wiadomości, wraz z ewentualnymi załącznikami, zawiera informacje przeznaczone tylko dla wymienionego w niej adresata i może zawierać informacje, które są poufne oraz prawnie chronione. Jeżeli nie są Państwo jej adresatem, bądź otrzymali ją przez pomyłkę należy: powiadomić niezwłocznie nadawcę poprzez odesłanie zwrotnej odpowiedzi na tą wiadomość, usunąć wiadomość w całości, nie ujawniać, nie rozpowszechniać, nie powielać i nie używać jej w jakikolwiek sposób w całości lub w części w jakiejkolwiek formie.

5. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji elektronicznej.

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

§ 7.1. 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 ABI, Administratorowi.

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

5. W Starostwie Powiatowym, zgodnie z zasadami organizacji pracy wydanymi przez Sekretarza Powiatu Łowickiego, w imieniu Administratora, klucze (3 komplety) do pomieszczeń są wydawane i odbierane przez upoważnione osoby. Klucze (jeden komplet znajduje się w gablocie) są pobierane przed rozpoczęciem pracy i zdawane po jej zakończeniu. Czynność ta jest odnotowana w książce pobieranych kluczy. Dwa komplety - zapasowy/ awaryjny znajduje się u dysponenta kluczy zapasowych i jest wydawany tylko w sytuacji awaryjnej. W przypadku wystąpienia sytuacji zagrożenia dyżurny, który jest pracownikiem biura ZK pobiera klucze z gabloty, fakt pobrania jest odnotowany w książce pobranych kluczy. Każde użycie klucza w przypadku awarii/zagrożenia wiąże się z koniecznością poinformowania Administratora i ABI.

6. Pomieszczenia, które są szczególnie istotne ze względu bezpieczeństwa informacji posiadają dodatkowe zabezpieczenia w postaci kodów dostępu oraz kart elektronicznych. Dostęp do tych pomieszczeń mają tylko osoby upoważnione. **Rejestr osób upoważnionych** jest prowadzony przez ASI/osobę wyznaczoną.

ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

§ 8.1. Osoba przetwarzająca dane, po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi, w specjalnie do tego przeznaczonych zamykanych szafach lub pomieszczeniach.

2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów.

3. Każdy dokument zawierający dane, a nieużyteczny 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

§ 9.1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić ABI, w razie jego nieobecności ASI.

2. W przypadku opisanym w ust. 1 ABI/ASI przeprowadza sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.

3. Przy dokonywaniu sprawdzenia ABI wykonuje działania:

1) **utrwala dane** z systemu informatycznego służącego do przetwarzania lub zabezpiecza na informatycznym nośniku dane lub dokonuje wydruku tych danych;

2) **odbiera wyjaśnienia osoby**, której czynności objęto sprawdzeniem;

3) **sporządza kopię** otrzyma/nego/ych dokumentów;

4) **sporządza kopię** obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.

4. Wykaz przykładowych sytuacji stanowiących naruszenie przyjętych zasad bezpieczeństwa stanowi załącznik nr 8 ***Przykładowe incydenty ODO*** do polityki bezpieczeństwa. Jest to lista otwarta, ulegająca modyfikacji.

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

§ 10.1. Pracownik ma nadany dostęp do systemu informatycznego na podstawie złożonego wniosku przez kierownika do administratora sytemu informatycznego, nie wcześniej jednak, jak po:

1) **zapoznaniu się 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.

2. Wniosek jest przekazany do ASI drogą elektroniczną i powinien zawierać poprawną informację o profilu uprawnień i przyjętym zakresem obowiązków na danym stanowisku. Wzór wniosku stanowi załącznik nr 4 ***Wniosek o nadanie uprawnień*** do polityki bezpieczeństwa

3. Administrator systemu informatycznego realizuje otrzymany wniosek lub odmawia nadania uprawnień do systemu informatycznego w przypadku uchybienia wymogom określonym w pkt.2 lub powzięciu przed administratora systemu informatycznego podejrzeń, co do przekroczenia uprawnień wymaganych na danym stanowisku.

4. W przypadku, powzięcia podejrzenia co do przekroczenia uprawnień wymaganych na danym stanowisku, administrator systemu informatycznego jest obowiązany zgłosić ten fakt administratorowi bezpieczeństwa informacji.

5. W przypadku, nadania uprawnień wymagających logowania, administrator systemu informatycznego przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby

pierwszego logowania. ASI prowadzi ***Rejestr użytkowników*** w postaci elektronicznej lub papierowej.

POLITYKA HASEŁ

§11.1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.

2. Hasła 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, kto posiada dostęp do systemów informatycznego administratora danych jest obowiązany do:

1) **zachowania w poufności wszystkich swoich haseł** lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;

2) **niezwłocznej zmiany haseł** w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;

3) **niezwłocznej zmiany hasła tymczasowego**, przekazanego przez administratora systemu informatycznego;

4) **poinformowania administratora systemu informatycznego** oraz administratora bezpieczeństwa informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła;

5) **stosowania haseł o minimalnej długości 8 znaków**, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;

6) **stosowania haseł** nie posiadających w swojej strukturze części loginu;

7) **stosowania haseł** nie będących zbliżone do poprzednich (np.Tadeusz$2013 - Tadeusz$2014);

8) **zmiany wykorzystywanych haseł** raz na **30 dni**.

5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.

6. Zabronione jest:

1) **zapisywanie haseł** w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;

2) **stosowanie haseł** opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;

3) **używanie tych samych haseł** w różnych systemach operacyjnych i aplikacjach;

4) **udostępnianie haseł** innym użytkownikom;

5) **przeprowadzanie prób** łamania haseł;

6) **wpisywanie haseł „na stałe"** (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);

7) po trzykrotnym, błędnym wprowadzeniu hasła następuje automatyczna blokada dostępu, użytkownik jest zobowiązany zgłosić ten fakt do administratora systemu informatycznego w celu zresetowania hasła dostępowego.

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI

§12.1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych Administratora danych powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych. W celu kontroli użytkowników jest prowadzony ***Rejestr kluczy kryptograficznych***. Rejestr zawiera informację dot. użytkownika, w tym imię i nazwisko, stanowisko, data otrzymania klucza.

2. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji. Rejestr, o którym mowa w ust.1 wraz z ewentualnymi protokołami jest prowadzony przez ASI i stanowi dokumentację **Klucz kryptograficzny**.

3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (identyfikacji personalnej) przed dostępem osób nieupoważnionych.

4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnienie należy bezzwłocznie powiadomić administratora systemu informatycznego oraz administratora bezpieczeństwa informacji.

5. Dane osobowe wrażliwe lub informacje poufne administratora danych, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.

6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić administratorowi systemu informatycznego oraz administratorowi bezpieczeństwa informacji.

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

§13.1. 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.

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 danych.

5. Przed opuszczeniem miejsca 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 pracujący w systemie informatycznym, przetwarzając dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:

1) **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;

2) **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

§14.1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie administratora danych.

2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej administratora danych 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 administratora danych podlega rejestrowaniu i jest monitorowana. Informacje przesyłane za pośrednictwem sieci administratora danych (w tym do i z Internetu) nie stanowią własności prywatnej pracownika.

4. Wszelka korespondencja elektroniczna prowadzona przez użytkownika, a niezwiązana z działalnością administratora danych, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.

5. Użytkownicy mogą korzystać z systemu poczty elektronicznej dla celów prywatnych **wyłącznie incydentalnie.**

6. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez pracownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych lub umownych, a także na wydajność systemu poczty elektronicznej.

7. Zabronione jest:

1) **wysyłanie materiałów służbowych** na konta prywatne (np. celem pracy nad dokumentami w domu);

2) **wykorzystywanie systemu** poczty elektronicznej do działań mogących zaszkodzić wizerunkowi administratora danych;

3) **odbieranie przesyłek** z nieznanych źródeł;

4) **otwieranie załączników** z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;

5) **przesyłanie pocztą elektroniczną** plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;

6) **ukrywanie lub dokonywanie zmian** tożsamości nadawcy;

7) **czytanie, usuwanie, kopiowanie lub zmiana** zawartości skrzynek pocztowych innego użytkownika;

8) **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;

9) **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;

10) **wykorzystywanie poczty elektronicznej** do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora danych lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§15.1. 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 publicznej (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.

4. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące 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

§16. Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej administratora danych (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 danych;

2) **komputery przenośne** należy przewozić jako bagaż podręczny i w miarę możliwości je maskować;

3) **pracownik wykonując czynności zawodowe lub umowne w domu** 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;

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 administratora bezpieczeństwa informacji, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez administratora danych;

7) **problemy wynikające z nieprawidłowego** funkcjonowania sprzętu komputerowego należy zgłaszać administratorowi systemu informatycznego;

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§17.1. Do sprzętu komputerowego zalicza się między innymi:

1) komputery stacjonarne,

2) komputery przenośne,

3) tablety,

4) smartphony,

5) drukarki,

6) modemy,

7) monitory,

8) routery,

9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.

2. ASI 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 administratora bezpieczeństwa informacji.

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

§18.1. Każdy pracownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych u administratora danych, 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 Starostwie Powiatowym w Łowiczu 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

§19.1. Zidentyfikowanymi obszarami systemu informatycznego administratora danych narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.

2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.

3. Pracownik jako użytkownik systemu ma obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chce 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

§20.1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.

2. W sprawach nieuregulowanych w regulaminie lub polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.

3. W razie wątpliwości, co do właściwego przetwarzania oraz zabezpieczenia danych osobowych pracowników, interesantów, kontrahentów pytania należy kierować do ABI.

4. Przykładowy zakres i katalog spraw związanych z koniecznością informowania administratora bezpieczeństwa informacji określa załącznik ***Informowanie ABI*** do niniejszego Regulaminu

STAROSTA ŁOWICKI

Krzysztof Figat

Załącznik do Regulaminu ochrony danych
osobowych w Starostwie Powiatowym
w Łowiczu wprowadzony
Zarządzeniem Nr 18/2016
Starosty Łowickiego z dnia 21 marca 2016r.

Informowanie ABI

**w razie wątpliwości co do właściwego przetwarzania
oraz zabezpieczenia danych osobowych
pracowników, klientów lub kontrahentów
należy kierować pytania do ABI!**

SPRAWY PRACOWNICZE - Informujemy ABI o:

- zatrudnieniu nowego pracownika (osoby upoważnionej),
- zwolnieniu pracownika (osoby upoważnionej),
- skargach (związanych z przetwarzaniem danych osobowych) pracowników lub byłych pracowników,
- zamiarze udostępnienia danych osobowych pracowników podmiotom zewnętrznym.

PODMIOTY ZEWNĘTRZNE - Informujemy ABI o:

- zamiarze zawarcia umowy z podmiotem zewnętrznym (jeżeli umowa przewiduje przepływ danych osobowych),
- zamiarze zmiany podmiotu zewnętrznego przetwarzającego dane osobowe,
- postepowaniu przedstawicieli podmiotów zewnętrznych niezgodnym z zasadami bezpieczeństwa opisanymi na szkoleniu,
- przydzielaniu zdalnych dostępów do systemów informatycznych przedstawicielom firm zewnętrznych.

STRONY INTERNETOWE - Informujemy ABI o:

- zamiarze zmiany lub uruchomieniu nowego hostingu serwisów www zbierających lub przesyłających dane osobowe,
- zamiarze uruchomienia nowej strony internetowej lub modyfikowaniu funkcjonalności już istniejącej (jeżeli dochodzi do przepływu danych za ich pośrednictwem),
- zamiarze przetwarzania danych osobowych zgormadzonych za pośrednictwem stron internetowych w innym celu niż to wynika z „klauzul zgody",
- zamiarze umieszczenia (opublikowania) danych osobowych (w tym i zdjęć) na stronie internetowej.

DZIAŁANIA MARKETINGOWE - Informujemy ABI o:

- zamiarze zorganizowania konkursu, programu lojalnościowego lub innych działań marketingowych wymagających przetwarzania danych osobowych,
- zamiarze wysłania masowych informacji handlowych drogą elektroniczną lub prowadzenia telefonicznej kampanii marketingowej,
- zamiarze zakupu bazy danych osobowych,
- zamiarze nawiązania współpracy z podmiotem zewnętrznym w zakresie marketingu (związanym z przetwarzaniem danych osobowych).

USUWANIE DANYCH - Informujemy ABI o:

- zamiarze usunięcie większe ilości danych osobowych (zarówno wersja papierowa jak
  i system informatyczny),
- zamiarze przekazania nośników elektronicznych (komputerów/laptopów) zawierających dane osobowe podmiotom zewnętrznym (np. celem ich naprawy),
- niewłaściwym usuwaniu danych osobowych przez współpracowników (zwykłe śmietniki), zepsutym sprzęcie do niszczenia dokumentów.

INCYDENTY BEZPIECZEŃSTWA - Informujemy ABI o:

- wycieku, utracie (zagubieniu) lub udostępnieniu osobie nieupoważnionej danych osobowych,
- wycieku, utracie (zagubieniu) lub udostepnieniu osobie nieupoważnionej danych osobowych przez podmiot zewnętrzny (kontrahenta),
- nie działającym zabezpieczeniu danych osobowych (np. niszczarki do dokumentów, zgubione klucze, ujawnione i nie zmienione hasła dostępowe, etc.),
- nie stosowaniu się do procedur bezpieczeństwa (np. polityka czystego biurka, polityka czystego ekranu, polityka kluczy, etc.).

SKARGI I SYGNALIZACJE - Informujemy ABI o:

- wszelkich skargach osób fizycznych na niezgodne z prawem przetwarzanie danych osobowych,
- wszelkich pismach przychodzących z GIODO oraz innych organów państwa w zakresie ochrony danych osobowych,
- wszelkiej korespondencji przychodzącej od podmiotów zewnętrznych w zakresie wątpliwości (zgodności) działań z przepisami ochrony danych osobowych.

OKRESOWE KONTROLE

- współudział w okresowych kontrolach (sprawdzeniach) przestrzegania procedur opisanych w dokumentacji wewnętrznej,
- składanie wyjaśnień, udostępnianie dokumentów oraz systemów informatycznych do kontroli (sprawdzenia).

INNE SPRAWY

- zamiar przeprowadzki, uruchomienia lub zlikwidowania wydziału/ biura/ samodzielnego stanowiska w którym były przetwarzane dane osobowe.

Wszelkie propozycje zmian związanych z nadzorem prowadzonym przez ABI należy niezwłocznie zgłaszać do Starosty Łowickiego/kierownika oraz/ lub ABI

STAROSTA ŁOWICKI

Krzysztof Figat