STAROSTA NOWOTARSKI

Zarządzenie Nr 94/2014
Starosty Powiatu Nowotarskiego
z dnia 26 marca 2014 roku

W sprawie aktualizacji „Polityki bezpieczeństwa informacji w Starostwie Powiatowym w Nowym Targu" oraz „Instrukcji zarządzania systemami informatycznymi w Starostwie Powiatowym w Nowym Targu".

Na podstawie art. 36 ust.2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz.U. z 2002r. Nr 101, poz. 926 z póź. zm), oraz § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U z 2004r. Nr 100, poz. 1024) **zarządzam co następuje**:

§ 1

Dla zapewnienia ochrony przetwarzanych danych osobowych aktualizuje się:

1. „Politykę bezpieczeństwa informacji w Starostwie Powiatowym w Nowym Targu" stanowiącą załącznik Nr 1 do niniejszego Zarządzenia
2. „Instrukcję zarządzania systemami informatycznymi w Starostwie Powiatowym w Nowym Targu" stanowiącą załącznik Nr 2 do niniejszego Zarządzenia

§ 2

Powyższe dokumenty mają zastosowanie na wszystkich stanowiskach pracy, gdzie przetwarzane są dane osobowe lub praca odbywa się w systemie informatycznym Starostwa Powiatowego w Nowym Targu.

§ 3

Z treścią dokumentów o których mowa w § 1 Naczelnicy Wydziałów, osoby kierujące biurem zapoznają wszystkie podległe osoby zatrudnione przy przetwarzaniu danych osobowych i użytkowników systemu informatycznego.

§ 4

Traci moc Zarządzenie Nr 10/2013 Starosty Powiatu Nowotarskiego z dnia 6 lutego 2013r. w sprawie : wprowadzenia „Polityki bezpieczeństwa informacji w Starostwie Powiatowym w Nowym Targu" oraz „Instrukcji zarządzania systemami informatycznymi w Starostwie Powiatowym w Nowym Targu".

§ 5

Zarządzenie wchodzi z dniem podpisania.

STAROSTA
Krzysztof Faber

RADCA PRAWNY

Załącznik nr 1
do Zarządzenia Nr 94/2014
Starosty Powiatu Nowotarskiego
z dnia 26 marca 2014 roku

ZATWIERDZAM
STAROSTA
Krzysztof Faber
.....

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Nowy Targ - 2014

Spis treści:

Załączniki – zawierające wykaz zbiorów danych osobowych, programów zastosowanych do ich przetwarzania, opis struktury zbiorów danych osobowych, wskazujący zawartość poszczególnych pól informacyjnych, powiazania miedzy nimi oraz sposób przepływu danych pomiędzy systemami oraz obszar przetwarzania.

Rozdział 1 - Postanowienia ogólne

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych, jak również danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych w Starostwie Powiatowym w Nowym Targu. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Starostwa. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Cele i strategie bezpieczeństwa

1. Polityka bezpieczeństwa informacji przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Targu, zwana dalej „Polityką", jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:
   - tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych,
   - w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. Starostwo Powiatowe w Nowym Targu, realizując politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   - przetwarzane zgodnie z prawem,
   - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami,
   - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3. Starostwo Powiatowe realizując Politykę systematycznie unowocześnia stosowane na jego terenie informatyczne, techniczne i organizacyjne środki ochrony tych danych w celu zabezpieczenia danych osobowych przed ich:
   - udostępnieniem osobom nieupoważnionym,
   - zbieraniem przez osobę nieuprawnioną,
   - przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych,
   - nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Polityka została opracowana zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 200 r. Nr 101, poz. 926 ze zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

5. Zakresem stosowania Polityka obejmuje wszystkich pracowników Starostwa oraz inne osoby mające dostęp do danych osobowych, w tym stażystów, praktykantów, osoby zatrudnione na podstawie umów cywilno - prawnych.

Definicje

1. Administrator Danych Osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Starosta Powiatu Nowotarskiego, który ponosi pełną odpowiedzialność wynikająca z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów znajdujących się w jego dyspozycji.
2. Administrator Bezpieczeństwa Informacji (ABI) - pracownik Starostwa wyznaczony przez Administratora Danych Osobowych do wdrażania oraz nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.
3. Administrator Systemu Informatycznego (ASI) – pracownik - informatyk odpowiedzialny za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych przetwarzanych w systemie informatycznym.
4. Administrator Informacji (AI) - to Kierownicy Pionów, Naczelnicy Wydziałów, w których przetwarzana jest dana grupa informacji.
5. Starostwo - Starostwo Powiatowe w Nowym Targu.
6. Użytkownik systemu - osoba posiadająca upoważnienie wydane przez ADO mająca z racji wykonywanych obowiązków dostęp do danych osobowych występujących w jednostce. Użytkownikiem może być pracownik Starostwa, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno - prawnej, osoba odbywająca staż lub praktykę.
7. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
8. Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) czy podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących rożne funkcje)
9. Przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie: zwłaszcza takie, które wykonuje się w systemach informatycznych
10. System informatyczny - to zespół współpracujących ze sobą: urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych.
    - urządzenie to rodzaj mechanizmu lub zespół elementów, przyrządów służących do wykonywania określonej czynności, ułatwiający pracę,
    - program to odpowiednio uporządkowana sekwencja instrukcji mająca na celu wykonywanie określonych zadań,
    - procedury przetwarzania informacji i narzędzia programowe to pojęcia, które powinny być utożsamiane z oprogramowaniem.

11. Zabezpieczenie danych w systemie informatycznym - to wdrożenie i eksploatacja stosownych środków technicznych programowych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
12. Bezpieczeństwo systemu informatycznego - wdrożenie stosownych środków administracyjnych, technicznych, programowych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych osobowych.
13. Poufność informacji - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy, mają dostęp do informacji.
14. Integralność informacji - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.
15. Dostępność informacji - rozumiana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to konieczne.

Rozdział 2 - Odpowiedzialność za bezpieczeństwo informacji

1. Administratorem Danych Osobowych (ADO) jest Starosta Nowotarski, który odpowiada za:
   - realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Danych,
2. Administratora Bezpieczeństwa Informacji (ABI) powołuje ADO, który odpowiedzialny jest za:
   - realizację ustawy o ochronie danych osobowych w zakresie dotyczącym ABI,
   - zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione, oraz że mogą one wykonywać wyłącznie uprawnione operacje,
   - zabezpieczenie obszarów przetwarzania danych osobowych w sposób uniemożliwiający dostęp do nich osobom trzecim,
   - zgłoszenie konieczności uzupełnienia zakresu czynności osoby zatrudnionej przy przetwarzaniu danych o zakres odpowiedzialności tej osoby za ochronę danych do AI,
   - weryfikację dopuszczenia użytkowników do przetwarzania danych,
   - zatwierdzanie decyzji AI o przyznaniu danemu użytkownikowi identyfikatora w danym systemie przetwarzania,
   - zatwierdzenie decyzji AI o przyznaniu danemu użytkownikowi praw dostępu do informacji chronionych w danym systemie przetwarzania,
   - powiadomienie ASI o zmianie uprawnień dostępu użytkowania do systemu,
   - prowadzenie rejestru osób dopuszczonych do przetwarzania danych osobowych,
   - przygotowanie dokumentów polityki bezpieczeństwa systemu informatycznego, służącego do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Targu,
   - zapoznanie pracowników zatrudnionych przy przetwarzaniu danych osobowych z przepisami ustawy o ochronie danych osobowych.
3. Administratorami Informacji (AI) są Kierownicy Pionów, Naczelnicy Wydziałów, w których przetwarzana jest dana grupa informacji, odpowiedzialni są za:
   - poprawność merytoryczną danych gromadzonych w zbiorach danych osobowych,
   - określenie miejsca przetwarzania, przechowywania, tworzenia i niszczenia informacji należącej do danej grupy,

- określenie budynków, pomieszczeń lub części pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe,
- określenie, które osoby i na jakich prawach mają dostęp do danych informacji,
- powiadomienie ABI o zakładaniu zbiorów danych na lokalnych urządzeniach komputerowych oraz w formie manualnej,
- pomoc ABI przy zgłoszeniu zbiorów danych do rejestracji do Generalnego Inspektora Ochrony Danych Osobowych,

Praca AI jest nadzorowana pod względem bezpieczeństwa informacji przez ABI.

4. Administrator Systemów Informatycznych (ASI) jest odpowiedzialny za:
   - bieżący monitoring oraz zapewnienie ciągłości działania systemu informatycznego,
   - instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   - instalacje i konfiguracje oprogramowania systemowego i sieciowego,
   - kontrola legalności oprogramowania,
   - konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane chronione przed nieupoważnionym do nich dostępem,
   - współpracę z dostawcami usług i sprzętu sieciowego, serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
   - weryfikacje możliwości integracji systemów informatycznych,
   - przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   - przyznawanie na wniosek Administratora Informacji, za zgodą ABI ściśle określonych praw dostępu do informacji w danym systemie.
5. Użytkownik jest odpowiedzialny za:
   - zachowanie szczególnej staranności przy gromadzeniu danych,
   - przetwarzanie danych zgodnie z prawem,
   - zadbanie by dane były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tym celami,
   - zadbanie by dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   - poprawne korzystanie z aplikacji zgodnie z powierzonymi obowiązkami służbowymi,
   - informowanie ASI o wszelkich nieprawidłowościach działania komputera, zainstalowanych na nim aplikacji oraz systemu operacyjnego,
   - ustalanie haseł oraz okresowej jego zmiany,
   - utrzymywanie w ścisłej tajemnicy haseł, którymi się posługuje,
   - zgłaszanie ASI awarii urządzeń komputerowych, oprogramowania systemowego, sieci komputerowej.

Polityka bezpieczeństwa określa:

1. Wykazy zbiorów danych osobowych z określeniem nazwy zbioru, jego formą, nazwą systemu informatycznego, nazwą komputera oraz obszarem przetwarzania danych przez poszczególne Piony, Wydziały oraz Biura w Starostwie Powiatowym, stanowiące kolejne załączniki do niniejszego dokumentu.
2. Opis struktury zbiorów danych wskazujący zawartość informacyjną, przepływ danych pomiędzy systemami oraz połączenie z siecią publiczną, stanowią załączniki do niniejszego dokumentu, aktualizowane są w przypadku zmian.

Rozdział 3 - Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Środki ochrony fizycznej:

1. Budynki Starostwa są zamykane po zakończeniu pracy, i dozorowane przez wyznaczone osoby i/lub system monitoringu.
2. Przebywanie w pomieszczeniach osób postronnych może odbywać się wyłącznie w obecności pracowników Starostwa.
3. W przypadku przebywania interesantów bądź innych osób postronnych monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
4. Do przebywania w pomieszczeniach serwerowni uprawnieni są: ASI i informatycy.
5. Przebywanie w pomieszczeniach serwerowni osób reprezentujących firmę zewnętrzną dopuszczalne jest tylko w obecności osób upoważnionych, o których mowa w pkt. 4.
6. Klucze, kody dostępu posiadają tylko osoby uprawnione.

Środki sprzętowe, informatyczne i telekomunikacyjne:

1. Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia powinien być zniszczony w sposób uniemożliwiający jego odczytanie, przy pomocy niszczarki.
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego urządzeniem UPS na wypadek zaniku napięcia albo awarii w sieci zasilającej.
3. Na stanowiskach pracy, w których przetwarzane są dane osobowe tworzone są kopie zapasowe dokumentów, za tworzenie których odpowiedzialny jest użytkownik systemu oraz ASI. Jeżeli do utworzenia kopii zapasowych, konieczne są uprawnienia administratora, użytkownik tworzy kopie zapasowe przy współpracy z ASI.
4. Na serwerach oraz poszczególnych stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Starostwa skanowana jest programem antywirusowym przed odczytaniem jej przez użytkowania.
5. Stanowiska komputerowe monitorowane są za pomocą programów monitorujących prace w systemie.

Środki ochrony w ramach oprogramowania systemu:

1. Bezpośredni dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla ASI.
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny z jakiego korzystają pracownicy Starostwa pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

Środki organizacyjne:

1. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy muszą być przeszkolone w zakresie obowiązujących przepisów o ochronie

danych osobowych (ABI), procedur przetwarzania danych (ABI), oraz poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym (ASI).
2. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
3. Wprowadzono Instrukcję Zarządzania Systemem Informatycznym służących do przetwarzania danych osobowych w Starostwie Powiatowym w Nowym Targu.
4. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych
5. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.
6. Określono sposób postępowania z nośnikami informacji.

Zasady bezpieczeństwa dla dokumentów papierowych

1. Należy chronić dokumenty papierowe zawierające dane osobowe przed ich fizycznym uszkodzeniem, zniszczeniem lub innymi czynnikami uniemożliwiającymi odczytanie lub odzyskanie informacji na nich zawartych
2. Dokumenty papierowe zawierające dane osobowe muszą być zabezpieczone przed zagrożeniem ze strony otoczenia (ogień, wyciek wody itp.)
3. Dokumenty te powinny być fizycznie chronione przed kradzieżą, zniszczeniem lub niewłaściwym używaniem. Wychodząc z pomieszczeń biura należy sprawdzić, czy są one zamknięte w odpowiednich szafach, zgodnie z zasadą „czystego biurka".
4. Wszystkie dokumenty papierowe zawierające dane osobowe muszą być oznaczone dla ich identyfikacji.
5. Każdy przeznaczony do usunięcia (wyniesienia, przekazania) dokument papierowy zawierający dane osobowe musi uzyskać pozwolenie ABI.
6. Utrata i kradzież dokumentów papierowych zawierających dane osobowe powinna być zgłaszana ABI.
7. Każdy dokument papierowy zawierający dane osobowe wygenerowany jako dokument roboczy należy na koniec pracy zniszczyć w niszczarce do papieru lub zamknąć w bezpiecznym miejscu uniemożliwiając dostęp osobom postronnym (np. szafa zamykana na klucz).

Rozdział 4 - Opis zdarzeń naruszających ochronę danych osobowych

1. Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych., jednakże występowanie w/w zagrożeń może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.
2. Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych),
3. Zagrożenia zamierzone - świadome i celowe działania powodujące naruszenie poufności danych, (zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
   - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do systemu z jego wnętrza,
   - nieuprawnione przekazanie danych,
   - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu)
4. Za naruszenie ochrony danych uważa się również stwierdzenie nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.:
   - niezabezpieczone pomieszczenia,
   - nienadzorowane, otwarte szafy, biurka, regały,
   - pozostawienie danych w nieodpowiednich miejscach - kosze, stoły itp.
5. Naruszenie lub podejrzenie naruszenia bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:
   - losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np. wybuch gazu, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
   - niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie silnego pola elektromagnetycznego,
   - awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
   - pojawienie się odpowiedniego komunikatu alarmowego,
   - podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
   - naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
   - pracy w systemie wykazującej odstępstwa uzasadniające podejrzenia przełamania lub zaniechania ochrony danych osobowych- np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
   - ujawnienie nieautoryzowanym osobom dostępu do kont systemu,
   - naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.)

Rozdział 5 - Przeglądy i aktualizacje Polityki

1. Polityka bezpieczeństwa podlega przeglądowi i ewentualnej aktualizacji nie rzadziej niż raz na dwa lata. Przeglądu dokonuje ABI.
2. Polityka bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:
   - likwidacji, utworzenia lub zmiany zbiorów danych osobowych,
   - zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji Polityki,
   - innych znaczących zmian dotyczących danych osobowych w funkcjonowaniu Starostwa
3. Aktualizacji Polityki dokonuje ABI, natomiast zatwierdzenia zaktualizowanej Polityki dokonuje Starosta Powiatu Nowotarskiego.
4. Aktualizacji Instrukcji zarządzania systemami informatycznymi dokonuje ASI po uzgodnieniu z ABI, zatwierdza Starosta Powiatu Nowotarskiego.

Opracowali:

Administrator Systemu Informatycznego

Administrator Bezpieczeństwa Informacji

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych
w Starostwie Powiatowym
w Nowym Targu
Beata Sięka