Załącznik Nr 5
do Polityki Ochrony Danych Osobowych
w Starostwie Powiatowym w Nowym Tomyślu

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

Przedmiot Instrukcji.

Przedmiotem Instrukcji jest określenie zagadnień związanych z bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych, w szczególności gromadzonych, transmitowanych i przechowywanych w systemach informatycznych, a także sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

Instrukcja określa w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym;
3) stosowane metody i środki uwierzytelnienia oraz procedury, związane z ich zarządzaniem i użytkowaniem;
4) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
5) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania;
6) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w § 1 pkt. 5 powyżej;
7) sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
8) udostępnianie danych osobowych;
9) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych;
10) przetwarzanie danych osobowych na laptopach;
11) przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż laptopy.

§ 2

Procedury nadawania, modyfikacji i anulowania uprawnień do przetwarzania danych osobowych w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Dostęp do systemu informatycznego (rozumiany również jako nadanie, odebranie lub zmiana uprawnień zarówno do oprogramowania stanowiskowego jak i sieciowego) nadawany jest użytkownikowi na wniosek KKO .
2. Uprawnienia w systemie informatycznym przyznawane użytkownikowi, wynikają z zakresu jego obowiązków i powinny być zgodne z upoważnieniem do przetwarzania danych osobowych.
3. Użytkownikom należy przyznawać minimalne uprawnienia, niezbędne do realizacji zadań, wynikających z ich zakresu obowiązków.
4. Wraz z przekazaniem do Wydziału Organizacyjnego „Informacji o przeprowadzeniu szkolenia", której wzór stanowi załącznik nr 4 do PODO, KKO jest zobowiązany wystąpić drogą do ASI o nadanie identyfikatora do systemu dla osoby upoważnianej, z podaniem programów i zasobów, których będzie używał pracownik upoważniony do przetwarzania danych osobowych.
5. ASI wprowadza nadany identyfikator do systemu dopiero po otrzymaniu potwierdzenia o podpisaniu upoważnienia do przetwarzania danych osobowych od wydziału ds. kadrowych Starostwa.
6. Informacja o ustaniu stosunku zatrudnienia lub zakończeniu przez użytkownika wykonywania prac, określonych umową zlecenia / umową o dzieło / o staż / praktykę powinna być przekazana niezwłocznie przez Wydział Organizacyjny Starostwa do ASI. W takim przypadku ASI natychmiast po otrzymaniu informacji Starostwa blokuje dostęp użytkownikowi do systemu.
7. Zmiana nadanych wprowadzeniem identyfikatora do systemu uprawnień jest możliwa na wniosek KKO przedstawiony ASI.
8. ASI przy realizacji zadań z zakresu dostępu do systemu informatycznego, a w zczególności przy zakładaniu konta o odpowiednim identyfikatorze, zabezpiecza je hasłem, tokenem lub kartą mikroprocesorową.
9. Konto użytkownika zostaje zablokowane przez ASI na polecenie ADO, lub na wniosek KKO lub z inicjatywy ASI w przypadku wystąpienia incydentu bezpieczeństwa.
10. W przypadku naruszania przez użytkownika zasad pracy w systemie informatycznym, ASI może zablokować konto do czasu wyjaśnienia nieprawidłowości. ASI o fakcie zablokowania konta informuje Administratora.
11. ASI dokonuje okresowych przeglądów kont użytkowników w celu wykrycia kont nieaktywnych.
12. Powyższe zasady obowiązują również osoby uzyskujące dostęp do danych osobowych na podstawie umowy zlecenia.

13. Prace związane z przetwarzaniem danych osobowych w systemie informatycznym, w związku z pracą w zespołach, komisjach powinna wykonywać osoba będąca pracownikiem Starostwa lub jednostek organizacyjnych Powiatu, która posiada już nadany identyfikator do pracy w systemie.

§ 3

Rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym.

1. Przyznanie uprawnień w zakresie dostępu do danych przetwarzanych w systemach informatycznych zarówno stanowiskowych jak i sieciowych polega na przypisaniu przez ASI w systemie dla upoważnionego użytkownika:
   a. Unikalnego identyfikatora i hasła lub unikalnego identyfikatora i przypisanej do niego karty mikroprocesorowej;
   b. wprowadzeniu do systemu zakresu dostępnych dla danego użytkownika danych i dopuszczalnych operacji.
2. Każdy z użytkowników systemu posiada własny identyfikator i hasło.
3. Ustanowione hasło dostępu, w sposób poufny ASI przekazuje użytkownikowi.
4. Hasło ustanowione podczas przyznawania uprawnień użytkownik jest zobowiązany zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.
5. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
6. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła, tokena lub karty mikroprocesorowej.
7. W przypadku anulowania uprawnień użytkownika jego identyfikator, token lub kartę mikroprocesorową należy niezwłocznie zablokować w systemie oraz unieważnić hasło użytkownika.
8. Za wdrożenie i nadzór nad przestrzeganiem procedury rejestracji uprawnień użytkowników w systemach odpowiedzialny jest ASI.

§ 4

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła, lub weryfikacji tożsamości użytkownika przy użyciu tokena lub karty mikroprocesorowej.
2. Zmiana hasła użytkownika jeśli pozwala na to aplikacja lokalna lub sieciowa następuje nie rzadziej niż co 30 dni.
3. Identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być on przydzielany innej osobie.
4. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł i ochronę swoich tokenów lub kart mikroprocesorowych.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
8. Przy wyborze hasła jeśli pozwala na to aplikacja obowiązują następujące zasady:
   a. minimalna długość hasła – 8 znaków,
   b. właściwa złożoność hasła - litery duże i małe oraz cyfry lub znaki specjalne.
9. Jeśli pozwala na to aplikacja zakazuje się stosowania haseł:
   a. które użytkownik stosował uprzednio (do sześciu haseł wstecz),
   b. będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
   c. analogicznych jak identyfikator,
   d. zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci itp.,
   e. stanowiących wyrazy słownikowe lub przewidywalne sekwencje znaków np. 12345678 lub abcdefgh.
10. W systemach umożliwiających zapamiętanie hasła nie należy korzystać z tego ułatwienia.
11. Powyższe reguły w zakresie haseł dotyczą obowiązków użytkownika systemu niezależnie od istnienia lub nie mechanizmów wymuszających (ułatwiających) ich stosowanie.

§ 5

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Przed rozpoczęciem pracy w systemie informatycznym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora i hasła lub identyfikatora i przypisanej do niego karty mikroprocesorowej lub tokena.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy

wykonać opcję wylogowania z systemu, zablokowania dostępu poprzez zabezpieczony hasłem wygaszacz ekranu lub zablokowanie, wylogowanie sesji użytkownika, np. poprzez użycie kombinacji klawiszy na klawiaturze komputera:

a. „Ctrl+Alt+Delete" i wybór polecenia „zablokuj ten komputer" lub „wyloguj",
b. „logo systemu Windows+L" dla zablokowania komputera.
c. usunięcie tokena

3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
4. Ustawienie monitora podczas pracy powinno uniemożliwić podgląd jakimkolwiek osobom nieupoważnionym jeśli pozwalają na to warunki.
5. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów.
6. Przypadki stwierdzenia nieprawidłowości w zakresie działania systemu należy zgłaszać do ASI, który po stwierdzeniu przypadku stanowiącego incydent bezpieczeństwa podejmuje działania.
7. Zabronione jest podejmowanie działań mogących stanowić zagrożenie dla systemu, a w tym:
   a. łamanie haseł,
   b. dokonywanie włamań na konta innych użytkowników,
   c. nieprawne uzyskiwanie dostępu do kont administracyjnych,
   d. zakłócanie działania usług,
   e. omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione),
   f. doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty,
   g. praca na koncie innego użytkownika.

§ 6

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. W celu zagwarantowania bezpieczeństwa danych przechowywanych w systemie wykonywane są ich kopie zapasowe, tj. kopie bezpieczeństwa oraz archiwalne.
2. Kopie zapasowe dotyczą zarówno aplikacji lokalnych jak i sieciowych

3. Za systematyczne przygotowanie kopii zapasowych odpowiada KKO. W przypadku aplikacji sieciowych za ich tworzenie odpowiada ASI. Mogą one być również wykonywane okazjonalnie przez użytkowników, w celu zabezpieczenia danych szczególnie istotnych dla działalności Starostwa.
4. Bazy danych, oprogramowanie oraz konfiguracja systemów powinny być zabezpieczone w postaci kopii bezpieczeństwa.
5. Należy wykonywać następujące kopie bezpieczeństwa:
   a. przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,
   b. przed dokonaniem zmian w programach (np. zmiana wersji),
   c. zgodnie z przyjętym harmonogramem, określonym indywidualnie przez każdego KKO w stosunku do kopii danych lokalnych i przez ASI w stosunku do kopii danych w aplikacjach sieciowych.
6. Oprócz kopii bezpieczeństwa wykonywane są okresowo kopie archiwalne istotnych dla działalności Starostwa danych.
7. Za wdrożenie i nadzór nad stosowaniem zasad i trybu wykonywania kopii zapasowych odpowiedzialny jest ASI.

§ 7

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

I. Kopie zapasowe.
   1. Kopie zapasowe należy przechowywać w warunkach gwarantujących brak dostępu do nich osób nieupoważnionych, tj. w zabezpieczonych pomieszczeniach, w sejfach lub szafach zamykanych na klucz.
   2. W przypadku wykonywania zabezpieczeń długoterminowych lub na nośnikach zewnętrznych, np. płytach CD, DVD nośniki te należy sprawdzać pod kątem ich dalszej przydatności oraz odtwarzalności.
   3. Kopie zapasowe należy usunąć niezwłocznie po upływie okresów przechowywania lub w przypadku ustania ich użyteczności.

II. Elektroniczne nośniki informacji.
   1. Dopuszcza się używanie służbowych elektronicznych nośników informacji, zwanych dalej nośnikami, w celu przenoszenia i archiwizowania danych osobowych, w tym płyt DVD, dysków zewnętrznych oraz nośników przenośnych typu pendrive.
   2. Należy unikać przechowywania danych osobowych na nośnikach.
   3. Zabronione jest używanie nośników do przenoszenia danych osobowych na prywatne komputery lub inne prywatne urządzenia mogące służyć do przechowywania danych.
   4. Zabronione jest przetwarzanie danych osobowych poza siecią lokalną starostwa i jednostek organizacyjnych Powiatu.

5. Nośniki, zawierające dane osobowe, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny. Za ich oznaczenie w podległej komórce organizacyjnej odpowiada KKO.
6. Nośniki, zawierające dane osobowe, podlegają szczególnemu nadzorowi i są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w zamykanych szafach biurowych lub kasetkach.
7. W przypadku zaistnienia okoliczności uzasadniających konieczność wyniesienia nośnika zawierającego dane osobowe poza obszar przetwarzania danych osobowych jego użytkownik zobowiązany jest uzyskania zgody Administratora oraz do zachowania szczególnej ostrożności i zabezpieczenia nośnika przed dostępem osób nieupoważnionych, utratą lub zniszczeniem (np. poprzez szyfrowanie nośnika).
8. Nośniki, zawierające dane osobowe, należy transportować w sposób bezpieczny (nie pozostawić ich w miejscach widocznych np. w samochodach, przypiętych do pasków itp.).
9. Nośniki, zawierające dane osobowe, przeznaczone do:
    a. likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    b. przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    c. naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora.

§ 8

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

1. Oprogramowanie stosowane, wdrażane, modyfikowane, zakupione w Starostwie może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych oraz powinno spełniać wymagania przepisów z zakresu ochrony danych osobowych.
2. Dozwolone jest jedynie uruchamianie oprogramowania związanego merytorycznie z wykonywaną pracą oraz dopuszczonego przez ASI do użytkowania w systemach Starostwa.
3. Korzystanie z zasobów informatycznych Starostwa poprzez sieć publiczną winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w szczególności firewall-i oraz systemu uwierzytelniania użytkowników i szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.
4. Sieć wewnętrzna Starostwa odseparowana jest od sieci publicznej za pomocą uaktywnionych firewalli sprzętowych lub programowych.

5. Dostęp do sieci wewnętrznej, przy zastosowaniu zasad dopuszczenia do zasobów informatycznych obowiązujących w Starostwa mogą posiadać:
   a. pracownicy Starostwa,
   b. osoby lub podmioty, z którymi Starostwa współpracuje na podstawie zawartych umów oraz ich pracownicy – w zakresie przewidzianym umową.
6. W celu ochrony systemów przed szkodliwym oprogramowaniem oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym systemu. Za prawidłowość realizacji powyższego obowiązku odpowiada ASI.
7. Sprawdzanie dostępności baz wirusów oprogramowania antywirusowego odbywa się automatycznie. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń.
8. Użytkownicy zobowiązani są do niezwłocznego zgłaszania do ASI każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów). ASI podejmuje działania mające na celu eliminację nieprawidłowości w zakresie realizacji obowiązku, o którym mowa w ust. 7 powyżej.
9. Programy antywirusowe winny być uaktywnione cały czas podczas pracy danego systemu.
10. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania szkodliwego oprogramowania najnowszą dostępną wersją programu antywirusowego. Pliki pochodzące z nośników zewnętrznych podlegają obowiązkowej kontroli pracowników ds. informatyki. Za przedstawienie do kontroli odpowiada KKO.
11. Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
12. Zabrania się używania elektronicznych nośników informacji niewiadomego pochodzenia.
13. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia otwierania podejrzanych wiadomości pocztowych (np. faktur, informacji o przesyłkach kurierskich oraz od nieznanych nadawców) .
14. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania, każdy użytkownik winien zawiadomić ASI o zaistniałym zdarzeniu.

§ 9

Udostępnianie danych osobowych.

1. Dane osobowe administrowane w Starostwie mogą być udostępniane:
   a. osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;
   b. innym osobom i podmiotom w przypadku posiadania przez wnioskującego podstaw do legalnego przetwarzania danych.
2. Udostępnienie danych nie może naruszać praw i wolności osób, których dane dotyczą.
3. W przypadku pojawienia się wątpliwości w zakresie możliwości udostępnienia danych osobowych Administrator zasięga opinii IOD.
4. IOD może wydać opinię negatywną udostępnienia danych jeżeli może to naruszyć bezpieczeństwo i ochronę danych zgromadzonych w systemie informatycznym.
5. W celu nadzoru nad udostępnianiem danych osobowych przypadki przekazania danych należy odnotowywać w systemach.
6. Dane udostępnione Starostwie przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

§ 10

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądy, konserwacje lub naprawy systemów i nośników wykorzystywanych w Starostwie dokonywane są przez osobę upoważnioną do tego typu czynności, w szczególności ASI.
2. Dopuszcza się realizację czynności określonych w ust. 1 przez specjalistyczne firmy świadczące usługi w tym zakresie; w takim przypadku konieczne jest zawarcie stosownej umowy cywilnoprawnej.
3. Umowy w zakresie świadczenia usług teleinformatycznych wiążące się z przetwarzaniem danych osobowych powinny być traktowane jako powierzenie przetwarzania danych osobowych.
4. Pracownicy firm świadczących usługi, o których mowa w ust. 2 powyżej wykonują zlecone zadania tylko za zgodą ASI, lub innego uprawnionego pracownika Starostwa i pod jego nadzorem.
5. W przypadku zdalnego dostępu do komputera lub fizycznej pracy osoby nie posiadającej uprawnień (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez ASI lub osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania.
6. Przeglądy i konserwacje wykonywane są cyklicznie oraz w przypadku pojawienia się usterki lub awarii systemów informatycznych.

§ 11

Przetwarzanie danych osobowych na komputerach przenośnych.

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
2. W sytuacji przetwarzania danych osobowych, przez pracowników Starostwa na komputerach przenośnych poza obszarem przetwarzania wskazanym w PODO, odpowiedzialni za ich bezpieczeństwo są ich użytkownicy i są zobowiązani chronić dane przed dostępem do nich osób nieupoważnionych.
3. Komputery przenośne po zakończonej pracy winny być przechowywane przez użytkownika w warunkach zapewniających ich bezpieczeństwo.
4. W przypadku korzystania z komputerów przenośnych poza obszarem przetwarzania należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby postronne.
5. Podczas transportu komputerów przenośnych wynoszonych poza obszar przetwarzania danych osobowych należy zapewnić ich bezpieczeństwo tj. nie należy ich pozostawiać bez nadzoru w samochodzie (lub innym miejscu). Muszą one być przewożone jako bagaż podręczny.
6. Należy unikać przechowywania na komputerach przenośnych danych osobowych.
7. Komputery przenośne muszą być wyposażone w uaktywniony firewall programowy.
8. W przypadku przetwarzania danych osobowych na komputerach przenośnych baza danych osobowych powinna być szyfrowana, zabezpieczona odpowiednim hasłem. Przetwarzanie danych na komputerach przenośnych poza obszarem przetwarzania odbywa się za zgodą Administratora.

§ 12

Przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż komputery.

1. Pracownicy korzystający z teleinformatycznych urządzeń przenośnych, tj. m.in. telefonów służbowych, tabletów, aparatów fotograficznych, kamer wideo, są zobowiązani chronić dane osobowe zawarte w pamięci tych urządzeń przed dostępem osób nieupoważnionych.
2. Wszelkie dane osobowe wprowadzone do pamięci urządzeń przenośnych powinny być usunięte przed zdaniem urządzenia do właściwej komórki organizacyjnej. Osobą właściwą do ich usunięcia jest pracownik lub funkcjonariusz korzystający z danego urządzenia. W

przypadku trudności technicznych przy usuwaniu danych osobowych należy kontaktować się z ASI.

3. Kontakt z serwisami zewnętrznymi, dotyczący użytkowanego sprzętu oraz oprogramowania, możliwy jest tylko za pośrednictwem ASI.

4. W treści informacji o przyznaniu pracownikowi urządzenia powinny znaleźć się wskazania w zakresie ochrony danych osobowych przetwarzanych przy jego pomocy.