Inwestuj

w kadry

Ochrona Danych Osobowych w praktyce - obowiązujące przepisy z uwzględnieniem nowelizacji.

Opracował: Marcin Sobota

Przepisy prawa w zakresie Ochrony Danych Osobowych

OBECNIE OBOWIĄZU JE:

Ustawa o ochronie danych osobowych.

Z DNIEM 25.05.2018 R. WCHODZI W ŻYCIE:

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Nowe przepisy wprowadzają nowe obowiązki wobec Administratorów Danych Osobowych. Zaliczyć do nich należy min. zasadę uwzględnienia ochrony danych osobowych w fazie projektowania, tzw. data protection by design w skrócie privacy by design.

Privacy by design wprowadza zasadę aby przewidywać zagrożenia jakie mogą pojawiać się przy przetwarzaniu danych osobowych przed ich zbieraniem.

RODO przewiduje karę za nie przestrzeganie privacy by design do 10 000 000 Euro lub 2 % całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego.

Privacy by design polega na:

- ✓działaniu zaradczym nie naprawczym,
- ✓prywatność jako działanie domyślne privace by default - oznacza zapewnienie ustawień zapewniających ochronę danych jako pierwotnych ustawień systemu informatycznego czy oprogramowania,
- ✓prywatność włączona w projekt privace embedded into desig,
- ✓pełna funkcjonalność,
- ✓pełna ochrona informacji w całym cyklu życia,
- ✓widoczność i przejrzystość,
- ✓poszanowanie dla prywatności użytkownika systemu.

Privacy by design została wdrożona w celu ochrony prywatności osoby fizycznej, której dane osobowe są przetwarzane przez administratorów danych.
Każdy ADO będzie musiał samodzielnie wdrożyć zasadę w swojej jednostce. Właściwym etapem wdrażania jest moment kiedy ADO ma zamiar rozpocząć zbieranie danych w określonym celu, np. akcja marketingowa. Drugim etapem privace by design jest etap realizacji procesu przetwarzania danych.

ADO lub ABI (Inspektor Ochrony Danych Osobowych) będą zobowiązani na każdym etapie przetwarzania do kontroli min. systemów informatycznych, sposobu zbierania zgód, wypełniania obowiązków informacyjnych.

Nie można zapomnieć również o zakończeniu procesu przetwarzania danych osobowych.
RODO wprowadza zasadę BYCIA ZAPOMNIANYM.

Ochrona danych osobowych wprowadza zatem konieczność ochrony prywatności osoby fizycznej również w kontekście właściwego zakończenia przetwarzania danych osobowych (informacji o osobie fizycznej).

Usunięcie danych osobowych wiąże się również z obowiązkiem informowania innych administratorów o procesie BYCIA ZAPOMNIANYM.

RODO wprowadza również pojęcie „BYCIA ZAPOMNIANYM”.

Polega ono na prawie żądania od administratora niezwłocznego usunięcia danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opierało się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych: z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na interesie publicznym lub prawnie uzasadnionych interesach i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania; lub wobec przetwarzania jej danych osobowych na potrzeby marketingu bezpośredniego;

RODO wprowadza również pojęcie „BYCIA ZAPOMNIANYM”

- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 GDPR.

Bycie zapomnianym wprowadza wobec administratorów dodatkowy obowiązek, mianowicie jeżeli administrator upublicznił dane osobowe ma obowiązek usunąć te dane, dotyczy to również sytuacji przekazania danych innym administratorom.

W przypadku przekazania danych osobowych innym podmiotom należy poinformować je, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Prawo bycia zapomnianym nie ma zastosowania w sytuacjach:

- korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- z uwagi na: cele zdrowotne oraz interes publiczny w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- do ustalenia, dochodzenia lub obrony roszczeń.

Przeciw działanie naruszeniom zasad przetwarzania danych osobowych;

- od 25 maja 2018 r. poza organami zajmującymi się ochroną danych osobowych również osoby, których dane dotyczą muszą uzyskiwać informacje o naruszeniu ich danych przy istnieniu tzw. przesłanki WYSOKIEGO RYZYKA.
- definicję naruszenia danych osobowych, zgodnie z RODO to: naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą to:

- uszczerbek fizyczny i szkoda majątkowa;
- naruszenie poufności danych objętych tajemnicą;
- utrata kontroli przez osobę nad jej danymi osobowymi;
- zagrożenie dla szczególnie chronionych kategorii danych, jak dane wrażliwe;
- ingerencja we wszelkie możliwe do zidentyfikowania aspekty osobiste w drodze profilowania.

„Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o powstaniu naruszenia, które może powodować wysokie ryzyko dla praw i wolności osób fizycznych”.

Zawiadomienie sformułowane musi być prostym językiem.
W zawiadomieniu muszą być zawarte informacje o:
- charakterze naruszenia,
- potencjalnych jego konsekwencjach,
- zastosowanych środkach,

zalecać działania zaradcze, które mogą zminimalizować negatywne konsekwencje naruszenia.
Administrator musi również poinformować osobę o danych kontaktowych inspektora ochrony danych lub punktu kontaktowego, gdzie będzie miała ona możliwość uzyskania dodatkowych informacji.

Obowiązek notyfikacyjny nie powstaje wówczas gdy po naruszeniu danych osobowych administrator zastosował odpowiednie środki techniczne o charakterze zabezpieczającym. Np. szyfrowanie, które uniemożliwiają dostęp do danych osobom nieupoważnionym.

Administrator nie ma również obowiązku notyfikacji w przypadku, kiedy wymagałoby to od niego niewspółmiernie dużego wysiłku. Wówczas powstaje alternatywa w postaci wydania publicznego komunikatu w tym zakresie.

Prawo do przenoszenia danych;

Prawo do przenoszenia danych osobowych przysługuje osobie, której dane dotyczą.
Zgodnie z nowelizacją prawa obowiązującą od dnia 25.05.2018 r.:

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

Prawo do przenoszenia danych;

Administrator jest zobowiązany przesłać te dane pod warunkiem, że:
- przetwarzanie odbywa się na podstawie zgody,
- dane przetwarzane są w sposób zautomatyzowany.

Osoba, której dane dotyczą ma prawo żądać aby dotychczasowy administrator przesłał je do nowego administratora (pod warunkiem istnienia możliwości technicznych).

Należy tu zauważyć, iż obecnie istniejące prawo do wglądu do swoich danych oraz prawo ich poprawienia zostaje poszerzone o prawo przeniesienia danych do innego administratora

Prawo sprzeciwu.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych, w tym profilowania.

Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Prawo sprzeciwu.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Prawo sprzeciwu.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Prawo sprzeciwu.

Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć prawo wnieść w dowolnym momencie, bezpłatnie sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego – w tym profilowania, o ile jest ono powiązane z marketingiem bezpośrednim. Prawo to powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji.

Profilowanie osób, których dane dotyczą.

Profilowanie klienta to np. kierowanie określonego rodzaju reklam do określonej grupy odbiorców. Profilowanie klienta to zbieranie informacji o zainteresowaniach np.. na podstawie plików „cookies”. Po wejściu w życie RODO osoby profilowane będą musiały zostać poinformowane o stosowaniu takiego mechanizmu i jego konsekwencjach. Na gruncie nowych przepisów osoba fizyczna zyska prawo do sprzeciwienia się profilowaniu. Oznacza to, że firma stosująca tego typu metody marketingowe, musi zapewnić takie mechanizmy, które będą umożliwiały wyłączenie z profilowania tych klientów, którzy sobie tego nie życzą.

Profilowanie osób, których dane dotyczą.

Informacja o profilowaniu musi być podana w sposób jasny i zrozumiały osobie, której dane są zbierane.

Profilowanie jest możliwe po zrealizowaniu obowiązku informacyjnego polegającego na:
- podaniu informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
- przedstawieniu istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,

Profilowanie osób, których dane dotyczą.

Jeżeli profilowanie nie jest niezbędne do wykonania umowy, nie ma swojej podstawy w przepisach prawa i nie jest dokonywane na podstawie zgody, oraz gdy decyzje podjęte w takim procesie opierają się na szczególnej kategorii danych (danych wrażliwych). W takiej sytuacji należy dodatkowo przekazać w ramach obowiązku informacyjnego:

- informacje o zasadach podejmowania takich decyzji (czyli w jaki sposób ta ocena następuje oraz przy pomocy jakich narzędzi będzie dochodzić do takiej oceny)
- informacje o znaczeniu i przewidywanych konsekwencjach dla osoby, której dane te dotyczą (tu chodzi o wyjaśnienie, jakie skutki prawne może nieść za sobą taka decyzja lub w jaki sposób prawnie będzie ta decyzja na daną osobę wpływać.

Profilowanie osób, których dane dotyczą.

Kolejnym obowiązkiem administratora danych jest umożliwienie podmiotowi danych wniesienia sprzeciwu wobec profilowania.

Obowiązek ten odnosi się do każdej kategorii profilowania (zarówno z udziałem czynnika ludzkiego, jak i zautomatyzowanego).

Profilowanie osób, których dane dotyczą.

Zgodnie z art. 4 pkt 4 RODO, profilowanie to:

„dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się”.

Dane osobowe wrażliwe:

Dane wrażliwe możemy podzielić na:
- dane ujawniające:
pochodzenie rasowe lub etniczne,
poglądy polityczne,
przekonania religijne lub filozoficzne,
przynależność wyznaniową, partyjną lub związkową,
- dane o:
stanie zdrowia,
kodzie genetycznym,
nałogach,
życiu seksualnym,
- dane dotyczące:
skazań, orzeczeń o ukaraniu i mandatów karnych,
innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie danych osobowych wrażliwych:

Przetwarzanie danych wrażliwych zwanych sensytywnymi, jest dopuszczalne,
Jeżeli:
1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi
o usunięcie dotyczących jej danych;
2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez
zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów
osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie
jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia
opiekuna prawnego lub kuratora;

Przetwarzanie danych osobowych wrażliwych:

4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;

5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;

6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;

Przetwarzanie danych osobowych wrażliwych:

7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;

8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej
przez osobę, której dane dotyczą;

Przetwarzanie danych osobowych wrażliwych:

9) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;
10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw
i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Upoważnienie do przetwarzania danych osobowych;

- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

- Administrator Danych lub Administrator Bezpieczeństwa Informacji jeśli został powołany, ma obowiązek „zapoznać osoby upoważnione do przetwarzania danych osobowych z przepisami o ochronie danych osobowych”.

- Upoważnienie do przetwarzania danych osobowych powinno być nadane w formie pisemnej lub elektronicznej.

- Zakres upoważnienia powinien odnosić się do zakresu faktycznie wykonywanych czynności na danych osobowych.

- Upoważnienie może być nadawane na czas określony lub nieokreślony (np.. na czas trwania stosunku pracy).

Wizerunek jako dana osobowa biometryczna;

- Wykorzystywanie wizerunku osoby fizycznej powinno następować za jej zgodą,

- Podmiot wykorzystujący wizerunek osoby fizycznej powinien wskazać w jakim celu i gdzie będzie on użyty,

- Art. 81 ustawy o prawie autorskim i prawach pokrewnych chroni wizerunek „wymaga zgody na rozpowszechnianie wizerunki osoby którą przedstawia, lub na którym osoba się znajduje.”

- Art. 81 ust. 2 wymienione są okoliczności kiedy wizerunek nie będzie chroniony przed upublicznieniem:
- wizerunek przedstawia osobę fizyczną w czasie wykonywania pełnionej funkcji publicznej, zwłaszcza politycznej lub samorządowej, społecznej lub zawodowej,
- osoba fizyczna jest elementem większej całości, np. w czasie imprezy masowej,
- lub osoba fizyczna jest tłem krajobrazu.

Wizerunek jako dana osobowa biometryczna;

- W przypadku monitoringu znajdującego się w budynku powinna znaleźć się informacja o dokonywanych nagraniach,

- Upowszechnianie wizerunku bez zgody osoby, której dotyczy jest naruszeniem prawa i podlega sankcją,

- Zdjęcie na którym jest uwidoczniona osoba fizyczna nie może w żaden sposób naruszać jej prawa do prywatności,

- Przy wykorzystywaniu zdjęcia, na którym uwidoczniona jest osoba fizyczna należy zwrócić uwagę na tzw. „pozowanie do zdjęcia" pozowanie oznacza bowiem świadomość bycia na fotografii.

Udostępnianie danych osobowych podmiotom trzecim.

Zgodnie z ustawą o ochronie danych osobowych przekazywanie danych podmiotom trzecim należy zaklasyfikować jako:
- ich udostępnienie
albo
- powierzenie ich przetwarzania.

Cecha, która różni te sposoby przekazania danych, to rola podmiotu, który dane osobowe otrzymuje. W przypadku udostępnienia danych osobowych ich odbiorca uzyskuje status administratora danych osobowych, podczas gdy przy powierzeniu przetwarzania pełni on funkcję wyłącznie podmiotu przetwarzającego dane na zlecenie ADO. Przykładem powierzenia danych osobowych może być np. korzystanie z serwera firmy informatycznej.

Udostępnianie danych osobowych podmiotom trzecim.

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Przetwarzanie danych osobowych.

Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Przetwarzanie danych osobowych.

Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych;

Dokumenty wewnętrzne związane z ochroną danych osobowych.

Podstawowym dokumentem związanym z ochroną danych osobowych w jednostce jest POLITYKA BEZPIECZEŃSTWA i INSTRUKCJA ZARZĄDZANIA SYSTEMAMI TELEINFORMATYCZNYMI

Dokumenty wewnętrzne związane z ochroną danych osobowych.

Dokument polityki bezpieczeństwa zawiera:

- Definicje bezpieczeństwa informacji, jego ogólne cela i zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji,

- Oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji,

- Krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań i zgodności mających szczególne znaczenie dla instytucji, np:
-zgodność z prawem i wymaganiami wynikającymi z umów;
-wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa
-zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania
-zarządzanie ciągłością działania biznesowego
-konsekwencja naruszania polityki bezpieczeństwa

Dokumenty wewnętrzne związane z ochroną danych osobowych.

- Definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania przypadków naruszenia bezpieczeństwa,

- Odsyłacze do dokumentacji mogącej uzupełniać politykę, np.: bardziej szczegółowych polityk bezpieczeństwa i procedur dla poszczególnych systemów informatycznych lub zasad bezpieczeństwa, których użytkownicy powinni przestrzegać,

- Wykaz zbiorów danych osobowych,

- Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe.

Dokumenty wewnętrzne związane z ochroną danych osobowych.

Opracowana instrukcja powinna zawierać:

- Zasady i procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie oraz wskazanie osoby odpowiedzialnej za te czynności,

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

- Procedury rozpoczęcia, zawieszenia i załączenia pracy przeznaczone dla użytkowników systemu ,

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

- Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego,

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

DZIĘKUJĘ ZA UWAGĘ