POLITYKA BEZPIECZEŃSTWA INFORMACJI

w

Laboratorium Kreatywności

01.05.2018 r.

Niniejsza *Polityka bezpieczeństwa*, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

Defnicje:

1. **Administrator Danych Laboratorium Kreatywności**
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych
5. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów
6. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych
7. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie
9. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

I Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w Laboratorium Kreatywności, niezale» nie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane s0 lub mog0 byĆ przetwarzane w zbiorach danych.

1. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.

2. Polityka jest udost4pniana do wgl0du osobom posiadaj0cym upowa» nienie do przetwarzania danych osobowych na ich wniosek, a tak» e osobom, kt..rym ma zostaĆ nadane upowa» nienie do przetwarzania danych osobowych, celem zapoznania si4 z jej tre, ci0.

3. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:

1. a) odpowiednie do zagro» e, i kategorii danych obj4tych ochron0 , rodki techniczne i rozwi0zania organizacyjne,
2. b) kontrol4 i nadz..r nad Przetwarzaniem danych osobowych,
3. c) monitorowanie zastosowanych , rodk..w ochrony.

4. Monitorowanie przez Administratora Danych zastosowanych , rodk..w ochrony obejmuje m.in. działania U» ytkownik..w, naruszanie zasad dost4pu do danych, zapewnienie integralno, ci plik..w oraz ochron4 przed atakami zewn4trznymi oraz wewn4trznymi.

5. Administrator Danych zapewnia, » e czynno, ci wykonywane w zwi0zku z przetwarzaniem i zabezpieczeniem danych osobowych s0 zgodne z niniejsz0 polityk0 oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone s0 w zbiorach danych.

2. Administrator danych nie podejmuje czynno, ci przetwarzania, kt..re mogłyby si4 wi0zaĆ z powa» nym prawdopodobie, stwem wyst0pienia wysokiego ryzyka dla praw i wolno, ci os..b. W przypadku planowania takiego działania Administrator wykona czynno, ci okre, lone w art. 35 i nast. RODO.

3. W przypadku planowania nowych czynno˙ ci przetwarzania Administrator dokonuje analizy ich skutk..w dla ochrony danych osobowych oraz uwzgl4dnia kwestie ochrony danych w fazie ich projektowania.

III. Obowi0zki i odpowiedzialno˙ Ść w zakresie zarz0dzania bezpiecze7 stwem

Wszystkie osoby zobowi0zane s0 do przetwarzania danych osobowych zgodnie z obowi0zuj0cymi przepisami i zgodnie z ustalon0 przez Administratora Danych Polityk0 Bezpiecze7 stwa, Instrukcj0 Zarz0dzania Systemem Informatycznym, a tak» e innymi dokumentami wewn4trznymi i procedurami zwi0zanymi z Przetwarzaniem danych osobowych w Laboratorium Kreatywności .

1. Wszystkie dane osobowe w Laboratorium Kreatywności s0 przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:

   a) W ka» dym wypadku wyst4puje chocia» jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.

   b) Dane s0 przetwarzane s0 rzetelnie i w spos..b przejrzysty.

   c) Dane osobowe zbierane s0 w konkretnych, wyrai nych i prawnie uzasadnionych celach i nieprzetwarzane dalej w spos..b niezgodny z tymi celami.

   d) Dane osobowe s0 przetwarzane jedynie w takim zakresie, jaki jest niezb4dny dla osi0gni4cia celu przetwarzania danych.

   e) Dane osobowe s0 prawidłowe i w razie potrzeby uaktualniane.

   f) Czas przechowywania danych jest ograniczony do okresu ich przydatno˙ ci do cel..w, do kt..rych zostały zebrane, a po tym okresie s0 one anonimizowane b0di usuwane.

   g) Wobec osoby, kt..rej dane dotycz0, wykonywany jest obowi0zek informacyjny zgodnie z tre˙ ci0 art. 13 i 14 RODO.

   h) Dane s0 zabezpieczone przed naruszeniami zasad ich ochrony.

2. Administrator danych nie przekazuje osobom, kt..rych dane dotycz0, in- formacji w sytuacji, w kt..rej dane te musz0 zostaĆ poufne zgodnie z obo- wi0zkiem zachowania tajemnicy zawodowej (art. 14 ust 5 pkt d RODO).

3. Za naruszenie lub pr..b4 naruszenia zasad przetwarzania i ochrony Danych osobowych uwa» a si4 w szczeg..lno˙ ci:

   a) naruszenie bezpiecze7 stwa System..w informatycznych, w kt..rych przetwarzane s0 dane osobowe, w razie ich przetwarzania w takich systemach;

   b) udost4pnianie lub umo» liwienie udost4pniania danych osobom lub podmiotom do tego nieupowa» nionym;

   c) zaniechanie, choĆby nieumy˙ lne, dopełnienia obowi0zku zapewnienia danym osobowym ochrony;

   d) niedopełnienie obowi0zku zachowania w tajemnicy Danych osobowych oraz sposob..w ich zabezpieczenia;

   e) przetwarzanie Danych osobowych niezgodnie z zało» onym zakresem i celem ich zbierania;

   f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;

   g) naruszenie praw os..b, kt..rych dane s0 przetwarzane.

4. W osobowych U» ytkownik zobowi0zany jest do podj4cia wszystkich niezb4dnych krok..w, maj0cych na celu ograniczenie skutk..w naruszenia i do niezwłocznego powiadomienia Administratora Danych,

5. Do obowi0zk..w Administratora Danych w zakresie zatrudniania, zako7 czenia lub zmiany warunk..w zatrudnienia pracownik..w lub wsp..łpracownik..w (os..b podejmuj0cych czynno˙ ci na rzecz Administratora Danych na podstawie innych um..w cywilnoprawnych) nale» y dopilnowanie, by:

   a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowi0zk..w,

   b) ka» dy z przetwarzaj0cych Dane osobowe był pisemnie upowa» niony do przetwarzania zgodnie z„Upowa» nieniem do przetwarzania danych osobowych" – wz..r Upowa» nienia stanowi Zał0cznik nr 2 do niniejszej Polityki Bezpiecze7 stwa,

c) ka» dy pracownik zobowi0zał si4 do zachowania danych osobowych przetwarzanych w kancelarii w tajemnicy. „O wiadczenie i zobowi0zanie osoby przetwarzaj0cej dane osobowe do zachowania tajemnicy" stanowi element „Upowa» nienia do przetwarzania danych osobowych".

1. Pracownicy zobowi0zani s0 do:

   a) cisłego przestrzegania zakresu nadanego upowa» nienia;

   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;

   c) zachowania w tajemnicy danych osobowych oraz sposob..w ich zabezpieczenia;

   d) zgłaszania incydent..w zwi0zanych z naruszeniem bezpiecze7 stwa danych oraz niewła ciwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w kt..rym przetwarzane s0 Dane osobowe na terenie Laboratorium Kreatywności obejmuje pomieszczenie biurowe kancelarii zlokalizowane w Bolesławcu 59-700 ul. Zgorzelecka 46.

2. Dodatkowo obszar, w kt..rym przetwarzane s0 Dane osobowe, stanowi0 wszystkie komputery przeno ne oraz inne no niki danych znajduj0ce si4 poza obszarem wskazanym powy» ej.

V. Okre lenie rodk..w technicznych i organizacyjnych niezb4dnych dla zapewnienia poufno ci, integralno ci i rozliczalno ci przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie rodk..w technicznych i organizacyjnych niezb4dnych dla zapewnienia poufno ci, integralno ci, rozliczalno ci i ci0gło ci Przetwarzanych danych.
2. Zastosowane rodki ochrony (techniczne i organizacyjne) powinny byĆ adekwatne do stwierdzonego poziomu ryzyka dla poszczeg..lnych system..w, rodzaj..w zbior..w i kategorii danych, rodki obejmuj0:

a) Ograniczenie dost4pu do pomieszcze7 , w kt..rych przetwarzane s0 dane osobowe, jedynie do os..b odpowiednio upowa» nionych. Inne osoby mog0 przebywaĆ w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upowa» nionej.

b) Zamykanie pomieszcze7 tworz0cych obszar Przetwarzania danych osobowych okre lony w pkt IV powy» ej na czas nieobecno ci pracownik..w, w spos..b uniemo» liwiaj0cy dost4p do nich os..b trzecich.

c) Wykorzystanie zamykanych szafek i sejf..w do zabezpieczenia dokument..w.

d) Wykorzystanie niszczarki do skutecznego usuwania dokument..w zawieraj0cych dane osobowe.

e) Ochron4 sieci lokalnej przed działaniami inicjowanymi z zewn0trz przy u» yciu sieci firewall.

f) Wykonywanie kopii awaryjnych danych na dysku przenośnym

g) Ochron4 sprz4tu komputerowego wykorzystywanego u administratora przed zło liwym oprogramowaniem.

h) Zabezpieczenie dost4pu do urz0dze7 Kancelarii przy pomocy haseł dost4pu.

i) Wykorzystanie szyfrowania danych przy ich transmisji.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodowaĆ ryzyko naruszenia praw lub wolno ci os..b zycznych.

2. W ka» dej sytuacji, w kt..rej zaistniałe naruszenie mogło powodowaĆ ryzyko naruszenia praw lub wolno ci os..b zycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zb4dnej zwłoki – je» eli to wykonalne, nie p..i niej ni» w terminie 72 godzin po stwierdzeniu naruszenia. Wz..r zgłoszenia okre la zał0cznik nr 3 do niniejszej polityki.

3. Je» eli ryzyko naruszenia praw i wolno ci jest wysokie, Administrator zawiadamia o incydencie tak» e osob4, kt..rej dane dotycz0.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych mo» e powierzyĆ przetwarzanie danych osobowych innemu

podmiotowi wył0cznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich um..w w art. 28 RODO.

2. Przed powierzeniem przetwarzania danych osobowych Administrator w miar4 mo» liwo, ci uzyskuje informacje o dotychczasowych praktykach procesora dotycz0cych zabezpieczenia danych osobowych.

VIII. Przekazywanie danych do pa7 stwa trzeciego

1. Administrator Danych Osobowych nie b4dzie przekazywał danych osobowych do pa7 stwa trzeciego, poza sytuacjami w kt..rych nast4puje to na wniosek osoby, kt..rej dane dotycz0.

IX. Postanowienia ko7 cowe

1. Za niedopełnienie obowi0zk..w wynikaj0cych z niniejszego dokumentu pracownik ponosi odpowiedzialno, Á na podstawie Kodeksu pracy, Przepis..w o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych obj4tych tajemnic0 zawodow0.
2. Integraln0 cz4, Á niniejszej Polityki bezpiecze7 stwa stanowi0 nast4puj0ce Zał0czniki:

Wz..r o, wiadczenia i zobowi0zania osoby przetwarzaj0cej dane osobowe

Wz..r upowa» nienia do przetwarzania danych osobowych.

Nazwa oraz dane kontaktowe Administratora Danych	Mariusz Potyszka Bolesławiec ul. Orląt Lwowskich 15 888999569
Imi4 i nazwisko lub nazwa oraz dane kontaktowe Inspektora Ochrony Danych Osobowych	
Opis kategorii os..b, kt..rych dane dotycz0, oraz kategorii danych osobowych	
Cele przetwarzania danych osobowych	Promocja Laboratorium Kreatywności
Kategorie odbiorc..w, kt..rym dane osobowe zostały lub zostan0 ujawnione, w tym odbiorc..w w pa7 stwach trzecich lub w organizacjach mi4dzynarodowych	
Informacja o przekazywaniu danych osobowych do pa7 stwa trzeciego	
Planowane terminy usuni4cia poszczeg..lnych kategorii danych	

Og..lny opis technicznych i organi zacyjnych ' rodk..w bezpieczeˀ stwa	

INSTRUKCJA ZARZ%DZANIA SYSTEMEM INFORMATYCZNYM

w

Laboratorium Kreatywności

01.05.2018 r.

Niniejsza *Instrukcja zarz0dzania systemem informatycznym słu» 0cym do przetwarzania danych osobowych*, zwana dalej Instrukcj0, przyj4ta została w celu wykazania, » e dane osobowe w systemach informatycznych Laboratorium Kreatywności przetwarzane s0 w spos..b zgodny z przepisami prawa maj0cymi zastosowanie do takiej czynno, ci, zgodnie z zasad0 art. 5 ust. 2 rozporz0dzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony os..b zycznych w zwi0zku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

1. **Administrator Danych Laboratorium Kreatywności**
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych
5. **SieÁ lokalna** – poł0czenie System..w informatycznych Administratora Danych wył0cznie dla własnych potrzeb przy wykorzystaniu urz0dze7 i sieci telekomunikacyjnych

1. **Zbi..r danych** – ka» dy posiadaj0cy struktur4 zestaw danych o charakterze osobowym, dost4pny według okre, lonych kryteri..w, niezale» nie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie
2. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udost4pnianie i usuwanie, a zwłaszcza te, kt..re wykonuje si4 w Systemach informatycznych
3. **Zabezpieczenie danych w systemie informatycznym** – wdro» enie i eksploatacja stosowanych , rodk..w technicznych i organizacyjnych zapewniaj0cych ochron4 danych przed ich nieuprawnionym Przetwarzaniem
4. **Identyfikator u» ytkownika** – ci0g znak..w literowych, cyfrowych lub innych jednoznacznie identy kuj0cy osob4 upowa» nion0 do Przetwarzania danych osobowych w systemie informatycznym (U» ytkownika) w razie Przetwarzania danych osobowych w takim systemie
5. **Hasło** – ci0g znak..w literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (U» ytkownikowi)

I. Procedury nadawania uprawnie7 do Przetwarzania danych i rejestrowania tych uprawnie7 w Systemie informatycznym

1. Za bezpiecze7 stwo Danych osobowych w Systemie informatycznym MAC OSX, Windows 10 i za wła, ciwy nadz..r odpowiedzialny jest Administrator Danych.
2. Do obsługi Systemu informatycznego oraz urz0dze7 wchodz0cych w jego skład, słu» 0cych do Przetwarzania danych, mog0 byÁ dopuszczone wył0cznie osoby posiadaj0ce pisemne upowa» nienie wydane przez Administratora Danych,
3. Po upowa» nieniu osoby do dost4pu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator u» ytkownika. Z chwil0 nadania Identyfikatora osoba mo» e uzyskaÁ dost4p do system..w informatycznych w zakresie odpowiednim do danego upowa» nienia.
4. Dla ka» dego U» ytkownika Systemu informatycznego ustalony jest odr4bny Identyfikator i Hasło.
5. Identyfikator u» ytkownika nie mo» e byÁ zmieniany, a po wyrejestrowaniu U» ytkownika z Systemu informatycznego nie mo» e byÁ przydzielony innej osobie.
6. Identy kator osoby, kt..ra utraciła uprawnienia do dost4pu do Danych oso- bowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w kt..rym s0 przetwarzane, za, Hasło dost4pu zostaje uniewa» nione oraz zostaj0 podj4te inne działania niezb4dne w celu zapobie» enia dalszemu dost4- powi tej osoby do danych.

II. Metody i ' rodki Uwierzytelnienia oraz procedury zwi0zane z ich zarz0dzaniem i u» ytkowaniem

1. W Systemie informatycznym stosuje si4 Uwierzytelnianie na poziomie dost4pu do systemu operacyjnego. Do Uwierzytelnienia U» ytkownika na poziomie dost4pu do systemu operacyjnego stosuje si4 Hasło oraz Identy kator u» ytkownika.
2. Hasła u» ytkownik..w umo» liwiaj0ce dost4p do Systemu informatycznego utrzymuje si4 w tajemnicy r..wnie» po upływie ich wa» no' ci.
3. Minimalna długo' Á Hasła przydzielonego U» ytkownikowi wynosi 6 znak..w alfanumerycznych i 5 znak..w specjalnych.
4. Zabrania si4 u» ywania identfikatora lub Hasła drugiej osoby.
5. Dla ka» dej osoby, kt..rej Dane osobowe s0 przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:
    a) daty pierwszego wprowadzenia danych do systemu,
    b) identyfikatora U» ytkownika wprowadzaj0cego Dane osobowe do systemu,
    c) informacji o odbiorcach, kt..rym Dane osobowe zostały udost4pnione.

III. Tworzenie kopii zapasowych Zbior..w danych

1. Dla zabezpieczenia integralno' ci danych dokonuje si4 archiwizacji danych w systemach Laboratorium Kreatywności.

2. Do archiwizacji słu» y dysk zewnętrzny.

3. Wszystkie dane archiwizowane winny by Á identyfikowane, tj. zawiera Á takie informacje jak dat4 dokonania zapisu oraz identy kator zapisanych w kopii danych.

IV. Spos..b, miejsce i okres przechowywania elektronicznych no' nik..w informacji zawieraj0cych Dane osobowe oraz kopii zapasowych

1. No' niki z kopiami archiwalnymi powinny by Á zabezpieczone przed dost4pem do nich os..b nieupowa» nionych, przed zniszczeniem czy kradzie» 0.
2. No' nik..w z danymi zarchiwizowanymi nie nale» y przechowywa Á w tych samych pomieszczeniach, w kt..rych przechowywane s0 Zbiory danych osobowych u» ywane na bie» 0co.
3. No' niki informacji, kopie zapasowe, kt..re nie s0 przeznaczone do udost4pnienia, przechowuje si4 w warunkach uniemo» liwiaj0cych dost4p do nich osobom niepowołanym.
4. Kopie, kt..re s0 ju» nieprzydatne, nale» y zniszczy Á fizycznie lub stosuj0c wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania si4 wynoszenia jakichkolwiek nagranych no' nik..w zawieraj0cych

    dane osobowe z miejsca pracy.

V. Spos..b zabezpieczenia Systemu informatycznego przed działalno' ci0 wirus..w komputerowych, nieuprawnionym dost4pem oraz awariami zasilania

1. System informatyczny jest zabezpieczony przed działaniem oprogramowa- nia, kt..rego celem jest uzyskanie nieuprawionego dost4pu oraz przed działa- niami inicjowanymi z sieci zewn4trznej. Zabezpieczenie obejmuje:

2. U» ytkowany system jest automatycznie skanowany z cz4stotliwo¸ ci0 raz w tygodniu.
3. Aktualizacja bazy wirus..w odbywa si4 poprzez automatyczne pobieranie bazy wirus..w przez program antywirusowy.
4. Urz0dzenia i no¸ niki zawieraj0ce Dane osobowe przekazywane poza obszar, w kt..rym s0 one przetwarzane, zabezpiecza si4 w spos..b zapewniaj0cy poufno¸ Á i integralno¸ Á danych.
5. W przypadku wykrycia wirusa nale» y:
    1. a) uruchomiÁ program antywirusowy i skontrolowaÁ u» ytkowany system,
    2. b) usun0Á wirusa z systemu przy wykorzystaniu programu antywirusowego.

Je» eli operacja usuni4cia wirusa si4 nie powiedzie, nale» y:

3. a) zako7 czyÁ prac4 w systemie komputerowym,
4. b) odł0czyÁ zainfekowany komputer od sieci,
5. c) powiadomiÁ o zaistniałej sytuacji Administratora Danych lub ABI.

VI. Poczta elektroniczna

1. Pracownicy mog0 korzystaÁ z poczty elektronicznej w celach słu» bowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowi0zkami.
2. Administrator mo» e poznawaÁ tre¸ Á wiadomo¸ ci elektronicznych wykorzystywanych przez pracownik..w znajduj0cych si4 we wszystkich systemach Administratora.
3. Zabronione jest otwieranie wiadomo¸ ci e-mail pochodz0cych od nieznanego nadawcy b0di z podejrzanym tytułem (tzw. *phishing e-mail*). W szczeg..lno¸ ci zabronione jest otwieranie link..w b0di pobieranie plik..w zapisanych w ko- munikacji zewn4trznej od nieznanego nadawcy.

VII. Sposoby realizacji w systemie wymog..w dotycz0cych Przetwarzania danych

1. Informacje o odbiorcach danych zapisywane s0 w Systemie informatycznym, z kt..rego nast0piło udost4pnienie.
2. Informacja o odbiorcy danych zapisana jest w Systemie informatycznym przy uwzgl4dnianiu daty i zakresu udost4pnienia, a tak» e dokładnego okre¸ lenia odbiorcy danych.
3. Mo» liwe jest sporz0dzenie i wydrukowanie raportu zawieraj0cego, w po- wszechnie zrozumiałej formie, powy» sze informacje.

VIII. Procedury wykonywania przegl0d..w i konserwacji systemu oraz no¸ nik..w informacji słu» 0cych do Przetwarzania danych

1. Przegl0dy kontrolne, serwis sprz4tu i oprogramowania powinny byÁ dokonywane przez firmy serwisowe, z kt..rymi zostały zawarte umowy zawieraj0ce postanowienia zobowi0zuj0ce je do przestrzegania zasad poufno¸ ci informacji uzyskanych w ramach wykonywanych zada7 .
2. Przy dokonywaniu serwisu nale» y przestrzegaÁ nast4puj0cych zasad:

a) czynno¸ ci serwisowe powinny byÁ wykonywane w obecno¸ ci osoby upowa» nionej do Przetwarzania danych,

b) przed rozpocz4ciem tych czynno¸ ci dane i programy znajduj0ce si4 w systemie powinny zostaÁ zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewła¸ ciw0 zmian0,

c) prace serwisowe nale» y ewidencjonowaÁ w ksi0» ce zawieraj0cej rodzaj wykonywanych czynno¸ ci serwisowych, daty rozpocz4cia i zako7 czenia usługi, odnotowanie os..b dokonuj0cych czynno¸ ci serwisowych, tj. imienia i nazwiska, a tak» e os..b uczestnicz0cych w pracach serwisowych,

d) w przypadku prac serwisowych dokonywanych przez podmiot zewn4trz- ny, wymagaj0cych dost4pu do Danych osobowych, z podmiotem takim powinny zostaÁ zawarte stosowne umowy powierzenia danych

osobo- wych.