ProGloss

LAKIERNICTWO MEBLOWE

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH

ProGloss Karol Czarny

ul. Powstańców 127, 31-670 Kraków

kom.: +48 733 933 345

kontakt@progloss.pl

NIP: 6762283241

REGON: 121010513

Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych stanowi o wymogach, zasadach i regulacjach ochrony danych osobowych w ProGloss zwanej dalej Podmiotem, jak również określa procedury i zasady bezpieczeństwa informacji w Podmiocie. Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych Podmiotu została opracowana na zlecenie Administratora Danych Osobowych ProGloss, zwanego dalej Administratorem lub ADO, w celu spełnienia wymagań określonych w Rozporządzeniu 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).

Polityka Zarządzania Bezpieczeństwem Informacji i Ochrony Danych Osobowych, zwana dalej Polityką powstała w związku z wykorzystywaniem:

- danych osobowych w rozumieniu RODO,

- innych, niż dane osobowe, danych (informacji) podlegających ochronie,

- technologii informatycznych służących do realizacji zadań Podmiotu.

Odpowiedzialność:

• wdrożenie niniejszej Polityki - Administrator Danych Osobowych,

• stosowanie niniejszej Polityki – pracownicy Podmiotu przetwarzający dane osobowe,

• nadzór i monitorowanie przestrzegania niniejszej Polityki - Administrator Danych Osobowych.

Skróty i definicje:

Polityka oznacza niniejszą Politykę Bezpieczeństwa Informacji i Ochrony Danych Osobowych.

RODO oznacza Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679/UE z 27.04.2016 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) (Dz. Urz. UE L 119, s. 1).

Dane oznaczają dane osobowe.

Dane wrażliwe oznaczają dane specjalne i dane karne.

Dane specjalne oznaczają dane wymienione w art. 9 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 13 roku życia.

Osoba oznacza osobę, której dane dotyczą.

RCPD lub **Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

ADO / Administrator oznacza Administratora Danych Osobowych w Podmiocie, to jest ProGloss.

OGÓLNE CELE I ZAKRES ORAZ ZNACZENIE BEZPIECZEŃSTWA, JAKO MECHANIZMU UMOŻLIWIAJĄCEGO WSPÓŁUŻYTKOWANIE INFORMACJI

Celem zapewnienia bezpieczeństwa informacji jest w szczególności:

− ochrona zasobów informacji,

− zapewnienie ciągłości działania Podmiotu i sprawnej obsługi jego klientów i partnerów,

− zgodność procesu przetwarzania informacji z przepisami prawa,

− ochrona wizerunku Podmiotu.

Spełnienie powyższych celów poprzez zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności danych w ramach Polityki umożliwia współużytkowanie informacji.

Polityka jest w sposób ciągły aktualizowana tak, aby jej postanowienia odzwierciedlały zmiany prawa, bieżące wymogi techniczne jak i zmieniające się realia pracy Podmiotu.

Realizując Politykę w zakresie ochrony danych osobowych Podmiot dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia warunki, aby dane te były:

a) przetwarzane zgodnie z prawem,

b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnie z tymi celami,

c) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Realizując Politykę zapewnia się przetwarzanym danym:

a) poufność – informacja nie jest udostępniana ani ujawniana nieupoważnionym osobom czy podmiotom, tylko uprawnieni pracownicy mają dostęp do odpowiednich kategorii informacji,

b) integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany, zapewnia się dokładność i kompletność informacji oraz metod jej przetwarzania,

c) dostępność – istnieje możliwość wykorzystania informacji na żądanie, w założonym czasie, przez autoryzowany podmiot gwarantując zapewnienie, że tylko upoważnione osoby Podmiotu mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

d) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,

e) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,

f) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,

g) niezawodność – zamierzone zachowania i skutki są spójne.

Polityka ma również na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w zakresie:

a) naruszeń danych osobowych rozumianych, jako prywatne dobro powierzone Podmiotu,

b) naruszeń przepisów prawa oraz innych regulacji,

c) utraty lub obniżenia reputacji Podmiotu,

d) start finansowych ponoszonych w wyniku nałożonych kar,

e) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH

NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI PRZETWARZANIA DANYCH

W Podmiocie rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

Zabezpieczenia fizyczne:

• brama wjazdowa,

• pomieszczenia zamykane na klucz,

• szafy zamykane na klucz,

• alarm,

• zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej ,

• przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,

• przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.

Zabezpieczenia organizacyjne:

• Osobą odpowiedzialną za bezpieczeństwo danych jest ADO,

• ADO na bieżąco kontroluje prace systemu informatycznego z należytą starannością zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i obowiązującymi procedurami,

• Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania,

• Wykaz pracowników jednostki uprawnionych do przetwarzania danych osobowych,

• Przetwarzać dane osobowe mogą jedynie osoby posiadające stosowne upoważnienia ADO,

• W trakcie przetwarzania danych osobowych pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,

• W trakcie przetwarzania danych osobowych upoważniony pracownik Podmiotu winien dbać o należyte ich zabezpieczenie w tym w szczególności zabezpieczyć je przed możliwością wglądu bądź zmiany przez osoby do tego nieupoważnione,

• Po zakończeniu przetwarzania danych osobowych pracownik winien należycie zabezpieczyć przetwarzane przez niego dane w szczególności przed możliwością dostępu do nich osób nieupoważnionych.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH

OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

Obiekt Pomieszczenia, w których przetwarzane są dane: ProGloss Karol Czarny, ul. Powstańców 127/15

INFORMACJE O OKRESOWYCH ANALIZACH RYZYKA UTRATY INTEGRALNOŚCI,

DOSTĘPNOŚCI LUB POUFNOŚCI INFORMACJI

Utrzymanie bezpieczeństwa przetwarzanych przez Podmiot informacji rozumiane jest, jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot Polityki. Zarządzanie ryzykiem – rozumiane jest, jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych. Analizę ryzyka utraty integralności, dostępności lub poufności informacji przeprowadza się standardowo raz w roku oraz zawsze w przypadku wystąpienia jednej z poniższych sytuacji:

1) potwierdzenia wystąpienia incydentu bezpieczeństwa informacji – po zakończeniu czynności związanych z jego usunięciem,

2) wprowadzenia zmian w systemie informatycznym związanym z bezpieczeństwem informacji.

Ww. analizę przeprowadza ADO przy współpracy z wyznaczonymi przez ADO pracownikami Podmiotu.

Analizę ryzyka przeprowadza się zgodnie z obowiązującymi w Podmiocie zasadami zarządzania ryzykiem.

Administrator Danych Osobowych zapewnia także odpowiedni poziom bezpieczeństwa danych, w szczególności przeprowadza cyklicznie analizy ryzyka przetwarzania danych osobowych oraz oceny skutków ochrony danych osobowych. W tym celu kategoryzuje dane i czynności przetwarzania pod kątem szacowania ryzyka ich przetwarzania a także analizuje możliwe uchybienia i zagrożenia wynikające z przetwarzania danych uwzględniając zakres, cel i charakter ryzyka występowania w Podmiocie. Dodatkowo zarządza ryzykiem oraz zgłasza zidentyfikowane naruszenia danych osobowych do Urzędu Ochrony Danych Osobowych.

ZAKRES BEZPIECZEŃSTWA INFORMACJI

1. W systemie informacyjnym Podmiotu przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.

2. Informacje te są przetwarzane i składowane zarówno w postaci papierowej jak i elektronicznej.

3. Zakresy określone przez dokumenty Polityki mają zastosowanie do całego systemu informacyjnego Podmiotu, w szczególności do:

• wszystkich istniejących systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,

• wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,

• wszystkich pracowników i innych upoważnionych osób mających dostęp do informacji podlegających ochronie.

STRUKTURA DOKUMENTÓW

Dokumenty Polityki ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

Oprócz Polityki w zakresie ochrony danych osobowych w Podmiocie opracowano:

• Instrukcję zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisujących sposób zarządzania systemami przetwarzania danych osobowych,

• Instrukcję postępowania w sytuacji naruszenia danych osobowych opisującej tryb postępowania w sytuacji naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia a także uzasadnionego podejrzenia o przygotowanej próbie naruszenia.

Ponadto w Podmiocie przeprowadzono:

• Analizę konieczności wyznaczenia inspektora ochrony danych osobowych (inspektora IDO),

• Analiza podmiotu w zakresie posiadanych i przetwarzanych danych osobowych w obszarach:

✓ aspekty organizacyjne,

✓ aspekty przetwarzania danych przez osobę trzecią,

✓ aspekty organizacyjne – zakres ochrony danych osobowych,

✓ aspekty prawno-organizacyjne – zgody,

✓ aspekty techniczno-informatyczne.

DOSTĘP DO INFORMACJI

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Podmiocie zasad ochrony danych osobowych.

Zakres czynności osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

Pomieszczenia, w których są przechowywane dane osobowe, powinny być zamykane na czas nieobecności w nim osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

KOMPETENCJE I ODPOWIEDZIALNOŚĆ W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów lub pracownicza na zasadach określonych w kodeksie pracy.

ZARZĄDZANIE DANYMI OSOBOWYMI

Realizując politykę bezpieczeństwa informacji, ADO lub upoważniona przez niego osoba ma prawo wydawać instrukcje regulujące kwestie związane z ochrona danych w strukturach Podmiotu. W umowach zawieranych przez Podmiot winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnianych przez Podmiot. Ochrona danych osobowych Podmiotu, jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków jego pracowników.

ZASADY UDZIELANIA DOSTĘPU DO DANYCH OSOBOWYCH

Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami prawa oraz zasadami zawartymi w obowiązującej w Podmiocie Polityce i innych dokumentach czy procedurach wewnętrznych. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w pisemnym oświadczeniu, którego wzór stanowi załącznik nr 1 do niniejszej Polityki.

Dostęp do danych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ADO. Wzór upoważnienia stanowi załącznik nr 2 do niniejszej Polityki. Ewidencja upoważnień prowadzona jest przez ADO, która stanowi załącznik nr 3 do niniejszej polityki.

ADO może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników Podmiotu do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Podmiocie.

Przetwarzanie danych osobowych

Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach przez upoważnione do tego osoby.

Pomieszczenia są zamykane na klucz podczas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w sposób uniemożliwiający ich odczytanie.

Urządzenia lub dyski a także inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

Archiwizacji informacji zawierających dane osobowe odbywa się w formie elektronicznej oraz papierowej. Nośniki danych przechowywane są w wydzielonych pomieszczeniach, które zabezpieczone są przed dostępem osób nieupoważnionych.

ZASADY OGÓLNE W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

W PODMIOCIE

Administrator Danych Osobowych:

• dba o ochronę prywatności i przetwarza dane zgodnie z wymogami prawa,

• zapewnia odpowiedni poziom bezpieczeństwa danych stale podejmując działania w tym zakresie,

• dokumentuje sposób spełniania obowiązki ustawowych w zakresie ochrony danych osobowych,

• dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych,

• opracowuje i prowadzi Rejestr Czynności Danych Osobowych, którego celem jest możliwość pełnienia nadzoru i monitoringu nad procesami przetwarzania danych osobowych.

Dodatkowo Inspektor Ochrony Danych Osobowych:

• zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze Czynności Danych Osobowych,

• utrzymuje system zarządzania zgodami na przetwarzanie danych,

• inwentaryzuje dane na podstawie prawnie uzasadnionego interesu,

• spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania.

Administrator Danych Osobowych informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

Administrator Danych Osobowych informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

Administrator Danych Osobowych bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

Administrator Danych Osobowych na żądanie osoby informuje ją, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących.

Administrator Danych Osobowych dokonuje sprostowania nieprawidłowych danych na żądanie osoby.

Administrator Danych Osobowych uzupełnia i aktualizuje dane na żądanie osoby, ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania.

Administrator Danych Osobowych na żądanie osoby usuwa dane, gdy zajdzie choć jedna okoliczność wymieniona poniżej:

a.a.i.a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

a.a.i.b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

a.a.i.c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

a.a.i.d) dane były przetwarzane niezgodnie z prawem,

a.a.i.e) konieczność usunięcia wynika z obowiązku prawnego,

a.a.i.f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

Administrator Danych Osobowych zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

Administrator Danych Osobowych dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

Administrator Danych Osobowych dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

Administrator Danych Osobowych wdraża mechanizmy kontroli cyklu życia danych osobowych w Podmiocie, w tym weryfikacji dalszej przydatności danych względem terminów i punktów Kontrolnych wskazanych w Rejestrze.

ZASADY ZGŁASZANIA NARUSZEŃ BEZPIECZEŃSTWA INFORMACJI ORAZ ZAGROŻEŃ PRAWIDŁOWEJ REALIZACJI ZAŁOŻEŃ POLITYKI

1. Incydent naruszenia bezpieczeństwa informacji polega na udostępnieniu lub umożliwieniu dostępu osobie nieupoważnionej, nieuprawnionym ujawnieniu informacji, utracie, uszkodzeniu, zniszczeniu jej nośnika lub jakiegokolwiek elementu jej zabezpieczenia.

W szczególności incydentem naruszenia bezpieczeństwa informacji jest:

− nieautoryzowany dostęp do danych,

− nieautoryzowany dostęp do sytemu informatycznego,

− nieautoryzowana modyfikacja lub zniszczenie danych,

− nieautoryzowane udostępnienie danych,

− nielegalne ujawnienie danych,

− pozyskiwanie danych z nielegalnych źródeł,

− ujawnienie wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,

− kradzież nośników zawierających dane,

− rażące nieprzestrzeganie Polityki lub aktów prawnych regulujących zagadnienia bezpieczeństwa informacji oraz ochrony danych osobowych,

− wydarzenie losowe obniżające stan bezpieczeństwa systemu (brak zasilania, pożar itp.).

2. Każda osoba, która stwierdziła wystąpienie incydentu bezpieczeństwa informacji zobowiązana jest do stosowania procedur określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.

3. Administrator Danych Osobowych stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

INFORMACJE O ZASADACH PRZEPROWADZANIA KONTROLI ZGODNOŚCI SYSTEMU INFORMATYCZNEGO Z POLITYKĄ

a.a.i.f.a.i.1. Za kontrole zgodności systemu informatycznego z Polityką odpowiada ADO,

a.a.i.f.a.i.2. Termin, zakres i zasady przeprowadzania tych kontroli określa ADO.

INFORMACJE O OKRESOWYM AUDYCIE WEWNĘTRZNYM W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI.

1. Zgodnie z aktualnie obowiązującymi przepisami prawa zapewnia się przeprowadzenie corocznego audytu wewnętrznego w zakresie bezpieczeństwa przetwarzanych informacji.

2. Audyt, o którym mowa w punkcie 1 będzie przeprowadzany ……..

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

RCPD stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady rozliczności. Administrator Danych Osobowych prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

Rejestr Czynności Przetwarzania Danych Osobowych zawiera:

• nazwa czynności przetwarzania,

• cel przetwarzania,

• kategorie osób,

• kategorie danych,

• planowany termin usunięcia kategorii danych,

• nazwa współ administratora i dane kontaktowe,

• nazwa podmiotu przetwarzającego i dane kontaktowe,

• kategorie odbiorców,

• ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

• transfer do kraju trzeciego lub organizacji międzynarodowej.

Wzór Rejestru Czynności Przetwarzania Danych stanowi załącznik nr 4 do niniejszej Polityki.

ZAPOBIEGANIE I WYKRYWANIE WIRUSÓW

ORAZ INNEGO ZŁOŚLIWEGO OPROGRAMOWANIA

W celu spełnienia wymogów Polityki w systemie informatycznym stosuje się ochronę przed wirusami i złośliwym oprogramowaniem poprzez rozwiązania organizacyjne oraz specjalne oprogramowanie. Poprawne działanie oprogramowania zależy zarówno od jego konfiguracji jak i od prawidłowych zachowań pracowników. Aby zagwarantować wysoki poziom ochrony, konieczne jest przestrzeganie następujących zaleceń:

1) Rozwiązania chroniące przed wirusami i złośliwym oprogramowaniem są zastosowane na każdym urządzeniu (systemie), które podatne jest na atak (uruchomienie) takiego oprogramowania.

2) Definicje służące do rozpoznawania nowych zagrożeń są wprowadzane w systemie niezwłocznie po ich upublicznieniu.

3) Jeżeli usunięcie wykrytego wirusa wymaga interakcji z użytkownikiem, użytkownik powinien proces usunięcia przeprowadzić zgodnie ze szczegółową instrukcją przygotowaną dla określonych przypadków.

4) Dane przechowywane na dyskach twardych powinny być sprawdzane zarówno w czasie rzeczywistym (przed każdym zapisaniem i odczytaniem) oraz okresowo w trybie dedykowanym, w którym sprawdzeniu podlegają jednocześnie wszystkie dane mogące zawierać wirusy.

5) Nośniki i dane pochodzące ze źródeł niegwarantujących ochrony przed wirusami muszą być sprawdzane przed ich wprowadzeniem do systemu Podmiotu. Sprawdzenie to jest wykonywane automatycznie, przez zainstalowane oprogramowanie.

6) Dane, które mogą zawierać wirusy, a do systemu docierają skompresowane lub zaszyfrowane, muszą być przed sprawdzeniem przywrócone do właściwej postaci. Przywrócenie to może przebiegać automatycznie.

7) Pracownikom nie wolno tworzyć, generować, kompilować, kopiować, rozpowszechniać, uruchamiać ani wprowadzać do systemu żadnego oprogramowania, które może się automatycznie powielać, niszczyć dane, zagrażać ich bezpieczeństwu lub w jakikolwiek sposób zakłócać działanie systemu informatycznego.

KONSEKWENCJE NARUSZENIA POLITYKI

1. Niestosowanie się do postanowień Polityki może pociągać za sobą konsekwencje dyscyplinarne z rozwiązaniem umowy o pracę / staż / praktykę włącznie i/lub konsekwencje prawne. Konsekwencje powinny być uzależnione od stopnia złej woli użytkownika, od powtarzania się naruszenia i od rodzaju zagrożenia dla bezpieczeństwa danych.

2. Naruszenie zasad Polityki przez użytkownika może być na wniosek ADO powiązane z natychmiastowym odebraniem dostępu do informacji.

3. Aby podkreślić wagę naruszeń bezpieczeństwa przez pracowników, każde takie naruszenie powinno powodować rozważenie roszczeń odszkodowawczych lub poinformowanie organów ścigania. Decyzję w tym zakresie podejmuje ADO.

POSTANOWIENIA KOŃCOWE

Niniejszy dokument stanowi najwyższej rangi dokument wewnętrzny Podmiotu w zakresie bezpieczeństwa informacji i ochrony danych osobowych przetwarzanych w systemie informatycznym i tradycyjnym. Jest dokumentem wiążącym dla wszystkich pracowników podmiotu, oraz innych osób z nim związanych i posiadających upoważnienia do przetwarzania danych a także innych podmiotów (stron trzecich) mających dostęp do danych przetwarzanych w Podmiocie na podstawie odrębnych umów, określających szczegółowe zasady korzystania z danych Podmiotu.

Informacje niejawne nie zostały objęte zapisami niniejszego dokumentu. Zasady ochrony informacji niejawnych reguluje ustawa o ochronie informacji niejawnych oraz wewnętrzne regulacje Podmiotu.

1. Niniejsza Polityka jest dokumentem opisującym spełnienie wymogów prawnych ogólnego rozporządzenia o ochronie danych RODO.

2. Dokumentacja Polityki Bezpieczeństwa względem RODO wchodzi w życie z dniem