Polityka bezpieczeństwa przetwarzania danych osobowych

Żłobek „uRodzinki” z siedzibą w Dominowie, ul. Rynek 3 lok. 1, gmina Głusk, prowadzonego przez uRodzinki Sp. z o.o. z siedzibą w Ćmiłowie 53, 20-388 Lublin

Spis treści

Informacje ogólne

§ 1

1.Polityka bezpieczeństwa przetwarzania danych osobowych, zwana dalej „Polityką” określa zasady zarządzania procesami przetwarzania danych osobowych oraz ich zabezpieczenia techniczne i organizacyjne, które mają zapewnić ochronę przetwarzanych danych osobowych i zagwarantowanie praw osób, których te dane dotyczą.

2.Polityka objęta jest tajemnicą służbową.

3.Politykę stosuje się do:

1)danych osobowych:

- przetwarzanych w systemach informatycznych;
- zapisanych na nośnikach informacji;
- przetwarzanych tradycyjnie;

2)informacji dotyczących bezpieczeństwa przetwarzania danych osobowych i procedur dla ich ochrony w systemach informatycznych oraz wdrożonych zabezpieczeń technicznych i organizacyjnych.

3.Zasady określone w Polityce oraz w dokumentach powiązanych obowiązują osoby zatrudnione i stale bądź czasowo współpracujące bez względu na zajmowane stanowisko, czy zakres powierzonych zadań, miejsce wykonywanej pracy oraz rodzaj przetwarzanych danych osobowych, czy wykorzystywane środki dla ich przetwarzania.

§ 2

Polityka składa się z dwóch części:

1) część pierwsza - opisuje organizację ochrony danych osobowych, procedury i obowiązki związane z zabezpieczeniem danych osobowych w ogólności;
2) część druga - "Instrukcja zarządzania systemem informatycznym" (dalej jako: "Instrukcja") opisuje procedury oraz środki zabezpieczeń, służące zapewnieniu bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, tj. w sposób całkowicie lub częściowo automatyzowany.

Część I.
Definicje i podstawy prawne

§ 3

Zawarte w Polityce definicje i skróty oznaczają:

1.Administrator Danych Osobowych, zwany dalej „ADO” – uRodzinki Sp. z o.o. z siedzibą w Ćmiłowie 53, 20-388 Lublin, w imieniu której działa Zarząd, tj. osoba/-y decydujące o sposobie i treści operacji przetwarzania danych osobowych, odpowiedzialna za zabezpieczenie lub zagwarantowanie (m.in. umowne) przetwarzania danych osobowych w systemie, zgodnie z zapisami Polityki, w tym "Instrukcji zarządzania systemem informatycznym",

2. Pełnomocnik - osoba/podmiot wyznaczona, której zostały powierzone określone zadania ADO (o ile zostanie powołana);
3. bezpieczeństwo przetwarzania danych osobowych – zachowanie poufności, integralności, rozliczalności, dostępności, autentyczności, ciągłości działania i niezawodności, w odniesieniu do systemu teleinformatycznego;
4. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zapisane w postaci papierowej lub na nośnikach danych; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
5. Prezes Urzędu Ochrony Danych Osobowych/ organ nadzorczy – właściwy organ nadzorczy w obszarze ochrony danych osobowych;
6. naruszenie ochrony danych osobowych (incydent) – zamierzone lub przypadkowe naruszenie zasad przetwarzania danych osobowych prowadzące do niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych, m.in. powstałe w skutek wadliwego działania systemów lub środków ochrony bądź niedochowania staranności lub ingerencji z zewnątrz;
7. poufność – właściwość zapewniająca, że dane osobowe są dostępne tylko osobom lub podmiotom upoważnionym;
8. przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
9. podmiot przetwarzający/przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
10. rozliczalność – właściwość zapewniająca, że jakiekolwiek działania lub czynności w stosunku do danych osobowych, w tym podejmowane w systemach informatycznych mogą zostać przypisane w sposób jednoznaczny tylko oznaczonemu podmiotowi - użytkownikowi;
11. system (tele)informatyczny/system – zespół współpracujących urządzeń, programów, procedur, w tym też system tradycyjny – dokumentacja w wersji papierowej w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego;
12. użytkownik systemu/ użytkownik – osoba upoważniona do bezpośredniego dostępu do danych osobowych, przetwarzanych w tradycyjnej formie, jak i w systemie informatycznym, która posiada ustalony identyfikator i hasło, m.in. pracownik lub zatrudniony/ współpracujący na innej podstawie niż umowa o pracę;
13. zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie;
14. odbiorca danych – każdy komu udostępniane są dane osobowe z wyłączeniem:
    -osoby, której dane dotyczą,
    -osoby upoważnionej do przetwarzania danych,

-podmiotu przetwarzającego w imieniu i na rzecz administratora,

-organów państwowych lub organów samorządu terytorialnego, których dane są udostępniane w związku z prowadzonym postępowaniem;

15. integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zamienione lub zniszczone w sposób nieautoryzowany;
16. pseudonimizacja – przetworzenie danych osobowych w taki sposób, że nie można ich już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

§ 4

Podstawy organizacji oraz zasady przetwarzania danych osobowych określają:

1) 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 sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej jako: RODO, ogólne rozporządzenie o ochronie danych, Dziennik Urzędowy UE z dnia 4 maja 2016 r., L 119).
2) ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz.U. z 2019r., poz. 1781) i inne akty związane z RODO;
3) zatwierdzone Kodeksy postępowania lub regulacje płynące z poddania się certyfikacji lub zatwierdzenia Kodeksu - w przypadku poddania się jego regulacjom.

Zadania i organizacja

§ 5

1. ADO zapewnia właściwą organizację ochrony danych osobowych dla zapewnienia bezpieczeństwa i zgodności przetwarzania danych osobowych z prawem, ich weryfikowalności i zbierania wyłącznie dla oznaczonych celów oraz ich merytorycznej poprawności i proporcjonalności w stosunku do celów ich gromadzenia, przez okres niezbędny dla realizacji celów przetwarzania. Powyższe oznacza:
   1) przetwarzanie danych zgodnie z prawem i w jego granicach;
   2) zbieranie danych dla oznaczonych, zgodnych z prawem celów i nie poddawanie ich dalszemu przetwarzaniu niezgodnie z tymi celami;
   3) merytoryczną poprawność i adekwatność w stosunku do celów, dla jakich dane są przetwarzane;
   4) przechowywanie danych w postaci umożliwiającej identyfikację osób, których dotyczą, wyłącznie w okresie niezbędnym do osiągnięcia celu przetwarzania;
   5) uwzględnienie praw osoby której dane są przetwarzane, w szczególności w zakresie prawa do informacji;
   6) bezpieczeństwo danych zapewniane przy użyciu środków technicznych i organizacyjnych, które zapewniają rozliczalność, integralność oraz poufność danych.

2.W przypadku powołania - Pełnomocnik, jest upoważniony do wykonywania zadań ADO, w zakresie koordynacji zadań związanych z ochroną danych osobowych.

§ 6

W przypadku, gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem zasad albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 7

1.Wyznaczony Pełnomocnik lub ADO realizuje zadania w zakresie zapewnienia zgodnego z prawem przetwarzania danych osobowych i ich należytego zabezpieczenia, w szczególności zaś:

a) opracowuje lub nadzoruje opracowania i aktualizowanie dokumentacji związanej z procesami przetwarzania danych osobowych, w tym w obszarze organizacji technicznych środków przetwarzania danych osobowych, systemów informatycznych i aplikacji oraz ich zabezpieczenia;
b) wydaje upoważnienia oraz zapoznaje osoby upoważnione do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
c) przygotowuje pisma, decyzje i opiniuje zamiar udostępniania, czy zawarcia umów o przetwarzanie danych oraz formułuje propozycje właściwych klauzul umownych lub postanowień oraz udostępnia dane i zawiera właściwe umowy;
d) prowadzi rejestry: czynności lub kategorii czynności przetwarzania, ewidencję upoważnień, zawartych umów przetwarzania danych i inną dokumentację, zgodnie z odpowiednimi przepisami;
e) organizuje szkolenia;
f) monitoruje komunikaty i ogłoszenia organu nadzorczego oraz podejmuje lub inicjuje działania dostosowujące do nich.

2.Dla realizacji przypisanych obowiązków ADO/Pełnomocnik:

a) ma prawo wydawać pisemne zalecenia, wytyczne i kontrolować ich wykonanie oraz żądać udzielenia niezbędnej pomocy, informacji lub wyjaśnień;

b) ma zapewnione stosowne środki techniczne i organizacyjne niezbędne dla realizacji przypisanych mu zadań;

c) ma prawo składać wnioski w zakresie zmian organizacyjnych, czy dotyczących środków ochrony;

§ 8

1. ADO realizuje lub zleca podmiotom trzecim obowiązki w obszarze teleinformatyki, w tym:
   1)administrację zasobami teleinformatycznymi i odpowiada za:
      a) konfigurację komputerów oraz aparatów telefonicznych i innych urządzeń do pracy,
      b) instalację i bieżącą aktualizację oprogramowania zainstalowanego na urządzeniach,

c) nadzór wykorzystania systemów komputerowych z uwzględnieniem zasad bezpieczeństwa oraz ochrony antywirusowej,
d) konfigurację kont pocztowych na urządzeniach użytkowników,

2) zabezpieczenie systemów przetwarzania danych osobowych i przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;
3) zapewnienie poufności, integralności, autentyczności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych;
3) zapewnianie ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym (aplikacjami) przetwarzającym dane osobowe;
4) reagowanie bez zbędnej zwłoki, w przypadku naruszenia ochrony danych osobowych;
5) podjęcie niezbędnych działań w odniesieniu do incydentów związanych z bezpieczeństwem systemów przetwarzania danych, ich skutków oraz podjętych środkach i czynnościach dla przywrócenia bądź zapewnienia bezpieczeństwa przetwarzania danych osobowych;
6) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z RODO, w aspektach domyślnej ochrony danych osobowych oraz ochrony przed naruszeniami;
7) instalację i konfigurację oprogramowania i sprzętu typu „standalone", sieciowego i serwerowego używanego do przetwarzania danych osobowych i zabezpieczającego dane osobowe przed nieupoważnionym dostępem;
8) zapewnienie, by używane oprogramowanie było na bieżąco aktualizowane oraz by system i poszczególne stacje były zabezpieczone przed obecnością i działaniem szkodliwego oprogramowania;
9) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych, w tym analizowanie i ewentualne zgłaszanie możliwości sięgania po środki i techniki wzmocnienia bezpieczeństwa danych osobowych, jak pseudonimizacja, czy rozdział baz danych;
10) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
11) zarządzanie dostępem oraz przyznawanie dostępu do danych osobowych w danym systemie;
12) świadczenie pomocy technicznej, diagnozowanie i usuwanie awarii sprzętu komputerowego i innych urządzeń, w tym peryferyjnych (o ile nie są objęte serwisem podmiotu trzeciego) lub systemu i jego elementów, służącego do przetwarzania danych osobowych oraz współpraca z firmami świadczącymi usługi pogwarancyjnego wsparcia;
13) wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego;

§ 9

1. ADO zapewnia stosowanie rozwiązań technicznych umożliwiających dostęp zdalny i transfer danych osobowych z zachowaniem zasad zachowania integralności, poufności i rozliczalności przetwarzanych danych osobowych.

2.Warunki i stosowane techniki zapewnienia dostępu do systemów informatycznych dla użytkowników zewnętrznych winny pozwalać na zachowanie zasad, o których mowa powyżej.

§ 10

Opis struktury zbiorów danych osobowych zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych, przetwarzanych w systemach informatycznych, zawarte są w dokumentacji oprogramowania lub wynikają z charakteru prowadzonych zbiorów.

Ogólne powinności użytkowników, warunki realizacji przetwarzania

§ 11

1.Użytkownicy zobowiązani są w szczególności do niżej powołanych działań oraz informowania Pełnomocnika lub ADO, a w razie ich nieobecności inne osoby wyznaczone o każdym przypadku naruszenia lub zagrożenia dla ochrony danych osobowych, tj.:
   1)postępowania zgodnie z Polityką, w celu zgodnym z realizacją obowiązków płynących z zatrudnienia oraz dbałości o zgodne z prawem przetwarzanie danych osobowych,
   2)zachowywania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia przy użyciu dostępnych technik zapewniających ich bezpieczeństwo oraz zachowywania się i podejmowania czynności, które nie będą tworzyć lub sprzyjać ryzyku nieuprawnionego dostępu, ujawnienia, zniszczenia lub zniekształcenia,
   3)nie pozostawiania informacji zawierających dane osobowe przy urządzeniach, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione,
   4)o ile jest to zasadne, przesyłania danych osobowych przy wykorzystaniu środków ograniczających możliwość ich odczytania przez osoby nieupoważnione, w szczególności przy użyciu technik szyfrowania lub pseudonimizacji.

§ 12

1. Dane osobowe mogą być przetwarzane wyłącznie w pomieszczeniach do tego przeznaczonych lub z wykorzystaniem odpowiednich środków zapewniających ich bezpieczeństwo.
2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz pomieszczenia techniczne.
3. Do pomieszczeń przetwarzania danych osobowych zalicza się:
   1) pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub obowiązki realizują osoby zatrudnione, w szczególności w zakresie administracji;
   2) pomieszczenia, w których przechowywane elektroniczne nośniki informacji, kopie zapasowe;
   3) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego;
   4) pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.

4. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób wyłączający możliwość dostępu do nich osobom nieupoważnionym.

§ 13

1.W przypadku zainstalowania monitoringu wizyjnego siedziby zachowuje się niżej wymienione zasady.
2.Dane gromadzone dzięki niemu służą zapewnieniu bezpieczeństwa osób i mienia ADO, ich przechowywanie jest ograniczone czasem niezbędnym dla weryfikacji ewentualnych zdarzeń mających znaczenie dla stwierdzenia stanu bezpieczeństwa osób i mienia oraz braku zagrożeń.
3.Informację o monitoringu umieszcza się przy wejściu. Niezależnie od tego informację o zakresie i celach monitoringu miejsc i osób umieszcza się w dokumentach opisujących organizację i porządek w miejscu pracy i zatrudnienia.

§ 14

1.W przypadku rozpoznania potrzeby, ADO lub Pełnomocnik zapewnia zamieszczanie informacji o ochronie danych osobowych, ich gromadzeniu i ich przetwarzaniu dla realizacji żądania/ w interesie podejmującego kontakt telefoniczny lub realizującego kontakt innym kanałem.
2.W przypadku realizacji komunikacji z ADO poprzez środki i kanały komunikacji za pośrednictwem mediów społecznościowych, informacje o treści danych osobowych ujawnione przez osobę nawiązującą kontakt, uznaje się za upublicznione. Stosowne informacje o tych aspektach - w miarę możliwości, jeśli nie powoduje to szczególnych utrudnień - zamieszcza się w takich mediach oraz na własnej stronie www.

Zasady udzielania upoważnień i kontroli ich aktualności

§ 15

1.Przed rozpoczęciem przetwarzania danych osobowych każdy Użytkownik powinien zostać przeszkolony przez Pełnomocnika lub ADO.
2.Szkolenie powinno obejmować następujące zagadnienia:
   1) przepisy o ochronie danych osobowych, w tym istniejących uregulowaniach wewnętrznych w tym Polityki,
   2) zasady przetwarzania danych osobowych oraz procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych;
   3) zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
   4) zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych,

-

5) zasady dostępu do i użytkowania pomieszczeń, w których przetwarzane są dane os obowe,
6) sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,
7) odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

3.Szkolenia powinny być powtarzane okresowo lub na żądanie.

§ 16

1.Przetwarzanie danych osobowych odbywa się w oparciu o upoważnienie do przetwarzania danych osobowych, wystawianego przez Pełnomocnika lub ADO oraz w oparciu o nadane uprawnienia, dostępu w zakresie odnoszącym się do systemów informatycznych o ile są takowe wykorzystywane.

2.Upoważnienie obok treści upoważnienia zawiera oświadczenie o znajomości Polityki oraz zobowiązanie do zachowania w tajemnicy danych osobowych, sposobu ich zabezpieczania oraz przetwarzania danych osobowych. Upoważnienie zamieszcza się w aktach osobowych lub stanowi element treści dokumentów związanych z zatrudnieniem.

Odpowiedzialność za przetwarzanie danych osobowych

§ 17

1.Niezależnie od powołania Pełnomocnika, ADO może wyznaczyć inne zatrudnione osoby jako odpowiedzialne za ochronę im przypisanych i przetwarzanych danych osobowych (zbiorów), na podległych im stanowiskach.

2.Do kompetencji tych osób należy:

1) zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;
2) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
3) realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane;
4) zapewnienie na żądanie uprawnionych osób, udostępnianie informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione;
5) zapewnienie złożenia przez pracowników i zatrudnionych oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych;
6) udostępnianie danych osobowych lub przekazywanie danych do przetwarzającego, zgodnie z prawem i ustalonymi zasadami oraz treścią umów;
7) takie organizowanie stanowisk pracy, by przetwarzane dane osobowe były zabezpieczone przed nieuprawnionym dostępem i nadzór nad utrzymaniem takiego stanu;
8) nadzorowanie oraz egzekwowanie stosowania odpowiednich zabezpieczeń danych osobowych i ich zbiorów, zapewnienia ich właściwej struktury oraz ograniczoności dostępu do pomieszczeń, w których są one przetwarzane i przechowywane;

-

9) nadzorowanie obchodzenia się z materiałami i dokumentami zawierającymi dane os obowe, w tym z ich niszczeniem oraz archiwizacją.

4.Osoba/podmiot zajmujący się dokumentacją związaną z zatrudnieniem sprawuje nadzór nad kompletnością akt pracowniczych w zakresie związanym z obowiązkami związanymi z danymi osobowymi i ich ochroną.

§ 18

1.Niezastosowanie się do wprowadzonej przez ADO Polityki oraz naruszenia zasad i procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 § 1 Kodeksu pracy lub zastosowaniem innych środków przysługujących Pracodawcy.

2.Niezależnie od rozwiązania stosunku pracy, osoby popełniające przestępstwo mogą być pociągnięte do odpowiedzialności karnej na podstawie m.in. art. 266 i art. 267 Kodeksu karnego lub innej wynikającej z właściwych przepisów.

Obowiązki związane z gromadzeniem/pozyskiwaniem danych osobowych, obowiązek informacyjny

§ 19

Dane osobowe przetwarzane przez ADO mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 20

1. Wyznaczone osoby są odpowiedzialne za poinformowanie osób, których dane osobowe pozyskują, podając lub umieszczając w widocznym miejscu informacje:
   a) dane ADO wraz z danymi kontaktowymi;
   b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
   c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
   d) prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią jeżeli przetwarzanie odbywa się na podstawie ich realizacji;
   e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   f) braku zamiaru przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (lub zmiany tej okoliczności);
   g) okresie, przez który dane osobowe będą przechowywane - precyzyjnie lub opisowo;
   h) informacje o prawie do dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   i) w przypadku przetwarzania na podstawie zgody - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   j) informacje o prawie wniesienia skargi do organu nadzorczego;

k) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

l) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o zasadach ich podejmowania oraz znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

ł)w przypadku zamiaru zmiany celu przetwarzania, w stosunku do którego dane osobowe zostały zebrane - informacje o tym innym celu oraz innych powyższych informacji, jeśli uległy zmianie;

- powyższe nie ma zastosowania, gdy: ■ osoba, której dane dotyczą, dysponuje już tymi informacjami;

2.W przypadku pozyskiwania danych osobowych nie od osoby, której dotyczą, obowiązek informacyjny obejmuje jeszcze informację o kategorii danych osobowych oraz źródle ich pochodzenia - wtedy obowiązek informacyjny realizuje się odpowiednio:

a) najpóźniej w ciągu miesiąca po pozyskaniu danych osobowych;

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu

- powyższy obowiązek nie ma zastosowania, gdy: osoba, której ■ dane dotyczą, dysponuje już tymi informacjami;

■ udzielenie informacji jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; ■ wynika z przepisu prawa.

3.Niezależnie od powyższych informacji przekazywanych przy pozyskiwaniu lub w związku z pozyskaniem, osoba której dane dotyczą ma prawo uzyskiwania tych samych informacji i informacji o działaniach podjętych w następstwie skorzystania z praw osoby której dane dotyczą wraz z kopią danych osobowych podlegających przetwarzaniu. Informacje te udostępnia się:

a) na piśmie lub elektronicznie;

b) w terminie miesiąca od otrzymania żądania;

c) bez pobierania opłat;

- chyba że żądania są nadmierne, nagminne i ewidentnie nieuzasadnione.

4.Wnioski w sprawie sprostowania danych osobowych, ograniczenia przetwarzania danych osobowych, sprzeciwu wobec przetwarzania danych osobowych i żądania usunięcia danych osobowych przekazuje się do Pełnomocnika lub osoby wyznaczonej.

Prawo do bycia zapomnianym

§ 21

1. Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych, a ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
   c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania w interesie publicznym lub w celach prawnie uzasadnionych interesów, ze względu na swą szczególną sytuację i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania - lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania na potrzeby marketingu bezpośredniego, co powoduje zaprzestanie takiego przetwarzania;
   d) dane osobowe były przetwarzane niezgodnie z prawem;
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega ADO;
2. Jeżeli ADO upublicznił dane osobowe, a wobec wyżej powołanego żądania, ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Uwzględnienie żądania skutkuje usunięciem danych, z zastrzeżeniem § 22 ust. 1;
4. Powyższe regulacje nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
   a) do korzystania z prawa do wolności wypowiedzi i informacji;
   b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania lub do wykonania zadania realizowanego w interesie publicznym;
   c) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile realizacja uprawnienia, uniemożliwi lub poważnie utrudniłaby realizację celów takiego przetwarzania;
   d) do ustalenia, dochodzenia lub obrony roszczeń.

§ 22

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być usunięte, przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą lub - w uzasadnionych przypadkach - odpowiednio zabezpieczone dalej przechowywane dla celów archiwalnych bądź statystycznych.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych/takich danych osobowych. Powyższe nie dotyczy realizacji żądań organów i sądów, dla których dokumenty i dane przekazuje się w niezmienionej formie.

Udostępnianie/przekazywanie danych osobowych

§ 23

1. Udostępnienie danych osobowych może nastąpić tylko osobom lub podmiotom uprawnionym do ich otrzymania, w innym przypadku następuje odmowa udostępnienia danych osobowych.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
   2) na podstawie przepisu prawa, na żądanie uprawnionego organu,
   3) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
   4) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające identyfikację i wyszukanie żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. Wniosek o udostępnienie przekazywany jest do właściciela zasobów danych osobowych/ właściwego kierownika/wyznaczonej osoby/pracownika/ ADO, który podejmuje decyzję o udostępnieniu i informuje o tym Pełnomocnika lub ADO oraz ewidencjonuje czynność, chyba że udostępnienie stanowi realizację zawartej umowy i dokumenty/informacje z tym związane umieszcza się w dokumentacji umowy.
6. Właściciel zasobów danych osobowych/ wyznaczona osoba/pracownik jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

Zasady powierzenia przetwarzania danych osobowych

§ 24

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z ADO lub świadczące usługi w swoim imieniu na rzecz ADO mają dostęp do danych osobowych przez niego przetwarzanych.
2. Powierzenie przetwarzania danych osobowych może się odbywać wyłącznie poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych.
3. Przekazywanie danych osobowych może mieć związek, m.in. z zadaniami realizowanymi przez dostawców usług IT, podmiotom świadczącym usługi księgowe, kurierom, bankom, firmom transportowym i innym podmiotom realizującym zadania na rzecz ADO.

§ 25

1. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się: 1) cel i zakres przetwarzania danych osobowych;
   2) obowiązek zachowania w tajemnicy danych osobowych, w tym także przez osoby którymi się posługuje podmiot przetwarzający;

3) ewentualne konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy;
4) obowiązek podjęcia środków zabezpieczających dane osobowe oraz obowiązek spełnienia wymagań określonych w przepisach prawa;
5) zasady współpracy przy wywiązywaniu się z obowiązków ADO związanych z odpowiadaniem na żądania osoby której dane są przedmiotem przetwarzania;
6) zasady korzystania z usług innego podmiotu przetwarzającego (podpowierzenie);
7) czas trwania umowy;
8) wymagane działania w momencie zakończenia umowy;
9) prawa do audytu i monitorowania działań związanych z ochroną danych osobowych;
10) proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych.

2. Umowę powierzenia przetwarzania danych osobowych innemu podmiotowi lub właściwe postanowienia umowy, gdy nie planuje się zawierania odrębnej umowy w tej materii, na wniosek właściwego właściciela zasobów przygotowuje, uczestniczy w uzgodnieniach i następnie rejestruje Pełnomocnik lub osoba wyznaczona w prowadzonym rejestrze, z zastrzeżeniem obowiązujących szczegółowych procedur współpracy i uzgadniania dokumentów.

Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

§ 26

1.Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych zarówno w przypadku naruszenia, jak i podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w systemach tradycyjnych.

2.Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się, w szczególności:
1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
2) nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu, w tym zniekształcenie lub utratę danych;
3) kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe.

3.W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych pracownicy, osoby zatrudnione i współpracujące zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Pełnomocnika/ADO i bezpośredniego przełożonego oraz podjęcie stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań mających na celu zapobieżenie pogłębienia stanu naruszenia, a dalej wykonywanie otrzymanych dyspozycji. W przypadku stwierdzenia naruszenia ochrony danych osobowych lub takiego ryzyka w stosunku do systemu informatycznego lub jego elementów i braku możliwości natychmiastowego skontaktowania się z ADO/Pełnomocnikiem - dopuszcza się wyłączenie urządzeń z zasilania.

4.Pełnomocnik lub ADO podejmuje działania mające na celu:

1) minimalizację negatywnych skutków zdarzenia;
2) zabezpieczenie dowodów zdarzenia;
3) wyjaśnienie okoliczności zdarzenia;
4) umożliwienie dalszego bezpiecznego przetwarzania danych.

5. Dla weryfikacji naruszenia ochrony danych osobowych Pełnomocnik ma prawo do podejmowania wszelkich działań, w szczególności:
1) żądania wyjaśnień od pracowników;
2) korzystania z pomocy konsultantów;
3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

6. W stosunku do każdego zgłoszonego incydentu Pełnomocnik lub wyznaczona osoba sporządza raport oraz formułuje wnioski, o których informuje ADO.

§ 27

1. W przypadku naruszenia ochrony danych osobowych, ADO lub w jego imieniu Pełnomocnik, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Pełnomocnik (z wykazaniem umocowania) lub ADO jako podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je właściwemu administratorowi.
3. Zgłoszenie musi co najmniej:
a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli informacji nie da się udzielić w tym samym czasie, wtedy udziela się je sukcesywnie bez zbędnej zwłoki.
5. Pełnomocnik dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania tego obowiązku.

§ 28

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Pełnomocnik, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2.Zawiadomienie to zawiera przynajmniej informacje i środki, o których mowa w paragrafie powyżej
3.Zawiadomienia nie stosuje się, gdy:
   a) wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   b) zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   c) wymagałoby ono niewspółmiernie dużego wysiłku - w takim przypadku wydaje się publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Rejestr czynności i kategorii czynności przetwarzania i ocena skutków dla przetwarzania danych osobowych

§ 29

1.ADO, Pełnomocnik lub osoba wyznaczona, prowadzi rejestr czynności przetwarzania danych osobowych. W rejestrze tym prowadzonym w formie pisemnej i elektronicznej, zamieszcza się następujące informacje:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe ADO;
   b) cele przetwarzania;
   c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   e) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   f) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
2.W przypadku, gdy ADO jest podmiotem przetwarzającym, wspomniany rejestr zawiera wzmiankę o tym charakterze oraz dane:
   a) imię i nazwisko lub nazwa oraz dane kontaktowe właściwego administratora, w imieniu którego działa ADO oraz inspektora ochrony danych tego administratora;
   b) kategorie przetwarzań;
   c) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
3.ADO lub Pełnomocnik udostępnia rejestr na żądanie organu nadzorczego.

§ 30

1.Jeżeli dany rodzaj przetwarzania, w szczególności w przypadku na przyszłość podejmowania nowych rodzajów działalności lub lub nowych operacji i ich metod związanych z przetwarzaniem danych osobowych – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Pełnomocnik lub ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych

osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:
   a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   b) przetwarzania na dużą skalę szczególnych kategorii danych wrażliwych
   c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
3. Obowiązek dokonania oceny skutków dla ochrony danych lub brak takiego obowiązku, może wynikać też z komunikatów organu nadzorczego.
4. Przeprowadzana ocena - o ile jest prowadzona - zawiera, co najmniej:
   a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania
   b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
   d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych.
5. Oceny skutków dla ochrony danych nie przeprowadza się w stosunku do operacji przetwarzania, których podstawą jest obowiązek prawny ADO lub realizacja zadania w interesie publicznym.
6. Analiza ryzyka stanowi załącznik.

Postanowienia końcowe Części I

§ 31

1. Polityka bezpieczeństwa informacji jest dokumentem wewnętrznym i jest objęta obowiązkiem zachowania poufności przez wszystkie osoby, którym zostanie ujawniona.
2. Zmiany i aktualizacje Polityki przeprowadza w miarę potrzeb. Politykę udostępnia się do wglądu w siedzibie ADO. W przypadku wprowadzenia w jej treści istotnych zmian, informuje się o nich lub prowadzi szkolenia.

Część II. Instrukcja zarządzania systemem teleinformatycznym – do odpowiedniego stosowania, w miarę wzrostu organizacji ADO

Uwagi wstępne i definicje

§ 1

1. Celem „Instrukcji zarządzania system teleinformatycznym" zwanej dalej „Instrukcją” jest określenie sposobów zarządzania systemem teleinformatycznym, służącym do przetwarzania

danych osobowych, tak w interesie i na rzecz samego ADO, jak i podmiotów na których rzecz świadczy usługi.

2. Niniejsza instrukcja określa zasady zarządzania i eksploatacji systemu informatycznego służącego do przetwarzania danych osobowych.
3. Przestrzeganie postanowień niniejszej Instrukcji służyć ma zapewnieniu poufności, integralności, dostępności i niezawodności przetwarzania danych w systemie.
4. Z zachowaniem definicji ujętych w Części I Polityki, ilekroć w Instrukcji powołuje się niżej przywołane definicje, rozumie się przez nie:
   1) hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
   2) identyfikator – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   3) nośnik informatyczny – płyta CD\DVD, pamięć USB typu FLASH, zewnętrzny dysk HDD lub inny nośnik, na którym zapisano w formie elektronicznej dane osobowe, w tym treść dokumentu, itp.
   4) poufność danych – właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom;
   5) raport – przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych osobowych;
   6) sieć publiczna, sieć telekomunikacyjna – sieć telekomunikacyjna w rozumieniu ustawy Prawo telekomunikacyjne;
   7) serwisant – firma lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego;
   8) system (tele)informatyczny administratora danych – sprzęt komputerowy i inne urządzenia (odpowiednio telefony), oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje, co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną ADO;
   9) teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
   10) uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu-Użytkownika;
   11) bezpieczeństwo systemu informatycznego – wdrożenie środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych osobowych przed ich udostępnianiem osobom nieupoważnionym, modyfikacją, zniekształceniem lub usunięciem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem przepisów prawa i niniejszej Polityki.

Ogólna charakterystyka

§ 2

1. System informatyczny daje możliwość ustalenia, kto, i z jakich programów/modułów/aplikacji korzystał. Ponadto system ten zapewnia odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu;

2. Odnotowanie informacji, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie treści wprowadzonych danych, w tym także dane w formie służącej przeniesieniu ich do innego administratora (prawo do przenoszenia).
4. System umożliwia też wprowadzenie informacji o żądaniach ograniczenia przetwarzania danych osobowych.

Prawa i obowiązki użytkownika

§ 3

1.Prawa i obowiązki użytkowników sieci teleinformatycznej:

1) użytkownicy mogą korzystać z następujących zasobów sieciowych:
   a) dostępu do Internetu,
   b) kont poczty elektronicznej,
   c) możliwości zmiany własnego hasła dostępu do poczty,
   d) dostępu do własnych zasobów sieci lokalnej.
2) użytkownicy są zobowiązani:
   a) do codziennego porządkowania zasobów swojej stacji roboczej, usuwanie plików zbędnych, zakładanie w określonym porządku katalogów i podkatalogów,
   b) sprawdzać funkcjonowanie systemu ochrony antywirusowej po uruchomieniu stacji roboczej,
   c) skanować zewnętrzne nośniki elektroniczne przed ich otwarciem,
   d) zgłaszać niezwłocznie uwagi w przypadku podejrzeń pojawienia się wirusa lub niepoprawnego działania sprzętu, aplikacji,
   e) dbać o bezpieczeństwo swoich zasobów komputerowych poprzez stasowanie odpowiednich haseł zabezpieczających dostęp do własnego komputera i nie przekazywanie ich osobom trzecim,
   f) zachować szczególną ostrożność przy pracy z pocztą elektroniczną. W przypadku jakichkolwiek wątpliwości, szczególnie w przypadku nieznanych i niezamawianych załączników poczty elektronicznej, zakazuje się ich otwierania, w razie wątpliwości należy skontaktować się z ADO; dozwolone jest przy tym przekazywanie danych osobowych tą formą, ale tylko jednostkowych, nie całych zbiorów (baz) lub znaczących ich części - takie przekazywanie winno wiązać się co najmniej z ustanowieniem hasła dla odczytu, które winno być przekazane innym kanałem komunikacji lub udostępnione dopiero na żądanie adresata, w przypadku otrzymania tą drogą poleceń

   od przełożonych (w szczególności dotyczących realizacji przelewów) zaleca się przeprowadzenie dodatkowej weryfikacji istnienia takiego polecenia.
3) użytkownikom sieci komputerowej nie wolno:

a) udostępniać swojego konta pocztowego osobom trzecim,
b) wykorzystywać swojego konta i dostępu do Internetu w celu ściągania nielegalnego oprogramowania i zasobów Internetu, które są potencjalnym zagrożeniem dla całej sieci komputerowej,
c) zachowywać się wobec innych użytkowników sieci lokalnej i Internetu w sposób odbiegających od przyjętych norm obyczajowych i moralnych oraz norm prawnych,
d) podejmować działania powodujące zakłócenia pracy sieci lokalnej.

§ 4

Zabrania się, bez zgody lub polecenia ADO:
1) samodzielnego instalowania oprogramowania zarówno licencjonowanego, jak i nielegalnego oraz darmowego oraz jego używania;
2) samodzielnego naprawiania uszkodzeń mechanicznych, związanych ze złym funkcjonowaniem zestawu komputerowego;
3) montażu i demontażu urządzeń komputerowych.

§ 5

1. Urządzenia przenośne oraz nośniki danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych.
2. Komputery przenośne należy przewozić w torbach do tego celu przeznaczonych (posiadających specjalną strefę chroniącą przed uszkodzeniami mechanicznymi).
3. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych, ani też w samochodach w widocznych miejscach.
4. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu, przy czym planuje się ograniczać wykorzystywanie urządzeń typu nośniki danych.
5. Szczególnej ostrożności wymaga wykorzystywanie komputerów przenośnych ADO w miejscach publicznych - jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, odbywa się w warunkach wyłączających ryzyko zapoznania się z danymi przez osoby nieupoważnione.
6. Niedozwolone jest udostępnianie jakimkolwiek osobom komputera przenośnego należącego do ADO.
7. W przypadku powierzenia użytkownikowi komputera przenośnego, w sytuacji, gdy rejestracja danych odbywa się na tym urządzeniu, o ile ustawienia nie realizują tej funkcji, należy przewidzieć konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na tym komputerze.

§ 6

1. Każdy pracownik/ użytkownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.

2. W obszarach, w których nie przetwarza się danych osobowych w systemach informatycznych przepisy niniejszej Instrukcji stosuje się odpowiednio.

Uwarunkowania pracy systemu

§ 7

1. Przed atakami z sieci zewnętrznej wszystkie komputery (w tym także przenośne) chronione są środkami dobranymi przez ADO lub Pełnomocnika, w szczególności poprzez wyłączenie uprawnień administratora dla użytkowników, co nie wyłącza zakazu pobierania z sieci jakiegokolwiek oprogramowania bez wiedzy ADO lub Pełnomocnika, z zastrzeżeniem kategorii użytkowników uprzywilejowanych.
2. Użytkownicy zobowiązani są do zwracania uwagi oraz informowania, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń i je przeprowadzać.

§ 8

1. System informatyczny posiada szerokopasmowe połączenie z Internetem.
2. Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.
3. Korzystanie z zasobów sieci wewnętrznej jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej.
4. Operacje za pośrednictwem rachunku bankowego może wykonywać wyłącznie uprawniony pracownik po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

§ 9

Dla zapewnienia ochrony danych i ich zbiorów, przy przetwarzaniu danych w systemie teleinformatycznym stosowane są środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności, w postaci:

a) zabezpieczeń technicznych, zasad organizacji, ochrony fizycznej lub dozoru:
– zbiory danych przechowywane są na serwerze, zlokalizowanych w wydzielonym pomieszczeniu; dostęp do tych pomieszczeń mają wyłącznie wyznaczone osoby;
– dostęp zdalny realizowany poprzez VPN;
b) zabezpieczeń systemu operacyjnego – zbiory przetwarzanych danych znajdują się na serwerze zarządzane przez system operacyjny odporny na większość popularnych włamań oraz wirusów ; dodatkowo dostęp jest chroniony przez system zapór firewall, wewnętrzne mechanizmy autoryzacji dostępu użytkowników do poszczególnych aplikacji;
c) zastosowano rozwiązania typu:
- UPS chroniące przed awarią zasilania, rozpatrywane będą także odrębne obwody zasilające;
- macierzy dyskowej w serwerze głównym w celu ochrony danych osobowych; - automatycznego sporządzania kopii zapasowych;

§ 10

1. Architektura systemu informatycznego oraz wzajemne powiązania, rodzaje tych powiązań logicznych i sprzętowych oraz protokołów komunikacyjnych stanowią tajemnicę jednostki.
2. Informacje służące do przetwarzania danych osobowych zapisywane są na dyskach serwera plików i chronione są mechanizmami uprawnień do plików i katalogów .

Procedura nadawania, rejestrowania, zmiany i odbierania uprawnień do przetwarzania danych w systemie informatycznym, osoby odpowiedzialne

§ 11

1. Dostęp do systemów informatycznych mogą posiadać:
   1) pracownicy – niezbędny do wykonywania powierzonych im czynności służbowych,
   2) wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – zakres konieczny do realizowania danej usługi lub wykonania określonych czynności w systemie.
2. Uprawnienia nadaje ADO lub Pełnomocnik.
3. Nadanie uprawnień związane jest z wydaniem osobie upoważnienia do przetwarzania danych osobowych, na wniosek przełożonego danego pracownika, a w przypadku osoby nie będącej pracownikiem na wniosek pracownika koordynującego działania osoby, dla której upoważnienie jest wydawane - lub bezpośrednio przez ADO lub Pełnomocnika.Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.
4. Zakres uprawnień winien być adekwatny do zakresu zadań wykonywanych przez użytkownika, nie może być on szerszy niż wynika to z realizowanych czynności.
5. Uprawnienia do przetwarzania danych osobowych w systemie wystawiane są w momencie zatrudniania (współ-)pracownika. ADO/Pełnomocnik winien być w stanie każdorazowo ustalić, w odniesieniu do indywidualnego użytkownika, poziom dostępu do zasobów.

§ 12

1.W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, ADO dokonuje nadania użytkownikowi identyfikatora, wygenerowania hasła oraz wpisania identyfikatora do ewidencji osób uprawnionych do przetwarzania danych osobowych w systemie.

2.Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.

§ 13

1.Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.

2.Dla zapewnienia realizacji nakreślonych celów:

1) użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku;
2) hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi;
3) użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
4) hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności;
5) zabronione jest przechowywanie haseł w widocznych miejscach, oraz umieszczanie haseł w automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

§ 14

1. Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego na jemu tylko znane. Identyfikator użytkownika w aplikacji jest tożsamy z tym jaki został mu przydzielony w sieci lokalnej.
2. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został uprawniony.
3. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonane przy użyciu jego identyfikatora i hasła.

§ 15

1. Wszystkie konta dostępowe do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator, który utracił ważność również nie może być ponownie przydzielony innemu użytkownikowi. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób uprawnionych do przetwarzania danych osobowych. Podstawę tworzenia loginu/identyfikatora jest imię i nazwiska użytkownika.
5. Użytkownicy powinni wybierać hasła unikatowe, trudne do ustalenia, w szczególności nie mogą to być imiona, nazwiska, ciągi takich samych znaków, znane daty jak urodzenia itp.
6. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
7. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
8. Należy unikać ponownego lub cyklicznego używania starych haseł.
9. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w oddzielnym miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
10. Rutynowe działania użytkownika nie powinny być prowadzone z wykorzystaniem kont uprzywilejowanych.

11. Udostępnienie hasła osobie postronnej należy traktować jako poważne naruszenie ochrony danych osobowych oraz obowiązków pracownika.
12. Hasła dostępu do aplikacji i do serwera z danymi w sieci lokalnej muszą spełniać poniższe warunki:
    a) posiadać długość co najmniej 8 znaków,
    b) zawierać litery małe i duże,
    c) zawierać cyfry lub znaki specjalne.
13. Hasło jest zmieniane przez użytkownika nie rzadziej niż co 30 dni lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanych.
14. Użytkownik zobowiązany jest do:
    a) nieujawniania hasła innym osobom, w tym innym użytkownikom,
    b) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
    c) niezapisywania hasła,
    d) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
    e) przestrzegania zasad dotyczących jakości i częstości zmian hasła,
    f) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez osoby postronne.
15. Użytkownik systemu w trakcie pracy w aplikacji może zmieniać swoje hasło dostępu.
16. Za tajność hasła osobistego odpowiada każdy pracownik, który zobowiązany jest do jego zmiany niezwłocznie po nabraniu podejrzeń o jego ujawnieniu.
17. Zmiana hasła nie powinna być zlecana innym osobom.
18. W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
19. Identyfikator i hasła dostępu do aplikacji ABSI przechowuje w sposób uzgodniony z Pełnomocnikiem.

§ 16

1 . Użytkownik, który jest w posiadaniu hasła, zobowiązany jest je zmieniać:
1) okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła);
2) w każdym przypadku ujawnienia lub podejrzenia, że doszło do ujawnienia hasła - o czym informuje ADO /Pełnomocnika.

2. W przypadku braku dostępu do konta chronionego hasłem, z którego korzystanie leży w obowiązkach użytkownika, występuje on o zmianę hasła, także w sytuacji:
1) zapomnienia/zgubienia hasła;
2) wygaśnięcia ważności hasła;
3) zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła; 4) braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

§ 17

1. Wyrejestrowania użytkownika z systemu informatycznego polegające na odebraniu uprawnień dostępu dokonuje ADO/ Pełnomocnik.

2.Wyrejestrowanie może mieć charakter czasowy lub trwały.

3.Wyrejestrowanie następuje poprzez:

1) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe);

2) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4.Czasowe wyrejestrowanie użytkownika z systemu informatycznego powinno nastąpić w razie:

1) nieobecności użytkownika w pracy trwającej dłużej niż 30 dni kalendarzowych; 2) zawieszenia w pełnieniu obowiązków służbowych.

5.Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:

1) wypowiedzenie lub rozwiązanie umowy o pracę/współpracę,

2) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych, 3) dłuższa nieobecność w pracy.

6.Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w którego ramach zatrudniony był użytkownik

§ 18

1. W przypadku zmiany zakresu obowiązków służbowych pracownika lub zakończeniem przez niego pracy oraz odpowiednio zmian w stosunku do innych zatrudnionych, cofa się lub wprowadza zmianę zakresu upoważnienia i poziomu uprawnień.
2. W przypadku anulowania/odebrania uprawnień użytkownika jego identyfikator niezwłocznie zostaje zablokowany w systemie informatycznym, w którym przetwarzane są dane osobowe a hasło unieważnione.
3. ADO/Pełnomocnik prowadzi rejestr użytkowników systemu, w którym odnotowuje imię i nazwisko, identyfikator, zakres uprawnień użytkownika oraz datę nadania, modyfikacji i anulowania uprawnień.

§ 19

W systemie informatycznym stosuje się uwierzytelnienie jednostopniowe na poziomie dostępu do konta lokalnego, natomiast dwustopniowego w odniesieniu do niektórych aplikacji/oprogramowania (np. program pocztowy, dyski w chmurze). ADO /Pełnomocnik może wprowadzić dostęp dwustopniowy do wszystkich zasobów.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy

§ 20

1.Przed przystąpieniem do pracy w systemie, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2.Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności dokumentów i wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich zamykanych szafkach.

§ 21

1.Rozpoczęcie pracy na poszczególnych stacjach roboczych następuje po włączeniu napięcia w listwie podtrzymującej napięcie lub tylko komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi, hasła i identyfikatora, w sposób minimalizujący ryzyko podejrzenia przez osoby trzecie.
2.Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać pogląd), wydruki leżące na biurkach oraz w otwartych szafach.
3.W systemach operacyjnych komputerów należy włączyć wygaszacz ekranu uruchamiający się po np. 15/30 minutach bezczynności. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła.
4.Obowiązuje zakaz sporządzania kopii całych zbiorów danych. Te mogą być kopiowane tylko przez ADO /Pełnomocnika lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych.
5.Zakończenie pracy na stacji roboczej następuje po zamknięciu sesji wszystkich aplikacji, a następnie prawidłowym wylogowaniu się użytkownika, wyłączeniu komputera i ewentualnie zasilania. Nieprawidłowym jest zaś wyłączanie komputera bez uprzedniego zamknięcia otwartych aplikacji.
6.Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawianie bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe, osób nieupoważnionych.

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

§ 22

W przypadku podjęcia decyzji o podstawowym przetwarzaniu danych osobowych w systemie informatycznym, a nie tradycyjnym - kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie pracownikowi.

§ 23

1.W systemie informatycznym wykorzystującym technologię klient-serwer, kopie zapasowe wykonuje się po stronie serwera w innych przypadkach na urządzeniach końcowych.
2.Dostęp do kopii bezpieczeństwa mają tylko osoby wyznaczone.
3.Pozostałe kopie tworzy się na oddzielnych nośnikach informatycznych.
4.Nośniki zawierające kopie zapasowe należy oznaczać, jako „Kopia zapasowa dzienna/ tygodniowa/ miesięczna” wraz z podaniem daty sporządzenia. Niszczenie nieaktualnych lub wadliwych winno przebiegać według ustalonej procedury.

§ 24

1.Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest ADO/Pełnomocnik.
2.Kopie zapasowe bazy danych osobowych wykonywane w cyklu dobowym za pomocą narzędzi archiwizujących, umieszczane są na serwerze sieciowym.
3.Kopie zapasowe baz danych i wybranych elementów systemu informatycznego sporządzane są automatycznie przynajmniej każdego dnia roboczego.
4.Pliki kopii zapasowych oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.
5.Nośniki z kopiami zapasowymi przechowywane są w pomieszczeniach serwerowni lub innych dostatecznie chronionych.
6.Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.
7.ADO/Pełnomocnik odpowiada za prowadzenie ewidencji lub procedury wykonywania kopii zapasowych.
8.Czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych może ulegać zmianie.
9.Okresowo dokonuje się sprawdzania przydatności kopii archiwalnych.
10.Sporządzone kopie zapasowe przechowuje się w zabezpieczonych pomieszczeniach, do których dostęp jest ograniczony, przy czym wprowadzone zostanie przechowywanie dodatkowej kopii poza siedzibą ADO.

§ 25

ADO odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią lub naruszeniem bezpieczeństwa systemu informatycznego. Po odtworzeniu systemu informatycznego należy przeprowadzić weryfikację poprawności działania systemu przed jego oddaniem do użytkowania.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

§ 26

1.Dane osobowe przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników.
2.Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji.
3.Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia i dostępu do nich przez osoby nieuprawnione.

4. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu.
5. Po okresie obowiązującego okresu przechowywania kopie podlegają likwidacji poprzez ich fizyczne zniszczenie, zgodnie z ustalonymi procedurami. O okresie przetwarzania decydują właściwe regulacje, w tym okres realizacji celu przetwarzania. Decyzję o możliwości usunięcia danych podejmuje ADO/ Pełnomocnik lub wyznaczona osoba.

§ 27

1. Dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych winny być umieszczane w odpowiednich folderach przestrzeni dyskowej serwerów, przydzielonych każdemu użytkownikowi. Użytkownicy są odpowiedzialni za realizację tych czynności.
2. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.

§ 28

Nośniki informatyczne z zaszyfrowanymi danymi osobowymi oraz pozostałe nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 29

1. Wykorzystywane oprogramowanie może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych, obowiązkowo posiadać łatwo dostępną informację o identyfikatorze, wersji i numerze licencji.
2. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
   1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku;
   2) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi;
   3) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
   4) podłączania komputerów do sieci zewnętrznych, niezabezpieczonych sieci publicznych, chyba że w uzasadnionych przypadkach i z zachowaniem szczególnej ostrożności (brak dostępu do sieci zabezpieczonej i przebywanie, np. w urzędach, hotelach).
3. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) oprogramowanie antywirusowe,
2) zaporę sieciową,
3) aktualizację oprogramowania systemowego,
4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

4. ADO/Pełnomocnik jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:
   1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych,
   2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych,
   3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych,
   4) weryfikację poprawności aktualizacji oprogramowania systemowego.

§ 30

1. Ochrona antywirusowa jest realizowana przez oprogramowanie antywirusowe instalowane na serwerze i/lub stacjach roboczych użytkownika.
2. Bazy wirusów programów antywirusowych są uaktualniane automatycznie lub po ich pojawieniu się.
3. Użytkownik systemu na stanowisku komputerowym, importując dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod katem możliwości występowania w nich wirusów.

§ 31

ADO/Pełnomocnik prowadzi analizy co do zasadności zakupu i wdrożenia specjalistycznego sprzętu i oprogramowania monitorującego wymianę danych na styku:
1) sieci lokalnej i sieci rozległej;
2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

§ 32

1. Połączenie lokalnej sieci komputerowej z Internetem jest kontrolowane poprzez sprzętowe urządzenia typu i funkcjach router/firewall stanowiących mechanizm łączący się bezpośrednio z Internetem na interfejsie zewnętrznym.Dopuszcza się inne zabezpieczenia/ konfiguracje sprzętowe i funkcjonalne.
2. Skaner antywirusowy poczty elektronicznej musi być stale włączony.
3. Oprogramowanie antywirusowe powinno być zainstalowane tak, aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.
4. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach informatycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
5. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
6. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów są instalowane automatycznie lub po ich otrzymaniu lub ściągnięciu.

7.W razie zainfekowania systemu ADO/Pełnomocnik odpowiada za usunięcie zagrożeń.
8.Stacja robocza, na której zostanie zlokalizowany wirus, jeśli dalsze pozostawienie jej w sieci zagraża innym stacjom roboczym lub nie spełnia norm bezpieczeństwa, może zostać odłączona.

Sposób realizacji wymogów odnotowywania informacji o odbiorcach dla każdej osoby, której dane osobowe są przetwarzane

§ 33

1.System informatyczny umożliwia automatycznie:
1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu;
2) sporządzenie i wydrukowanie raportu dla każdej osoby, której dane są przetwarzane w systemie:
a) zawierającego datę pierwszego wprowadzenia danych do systemu ADO;
b) zawierającego identyfikator użytkownika wprowadzającego te dane;
2.Odnotowanie informacji następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3.System informatyczny zapewnia udzielenie osobom, których dane są przetwarzane w systemie informacji, od kiedy dane są przetwarzane, treści tych danych, informacji o sposobie udostępniania danych a zwłaszcza o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.
4.W sytuacji braku możliwości rejestrowania czynności o których mowa w ust. 2 i 3, udostępnienie rejestruje się w odrębnych zestawieniach.

Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 34

1.Przegląd, konserwacja i naprawy systemów i nośników wykorzystywanych są dokonywane przez osobę upoważnioną do tego typu czynności pod nadzorem lub przez ADO.
2.Przeglądy i konserwacje urządzeń w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
3.Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy powiadomić Pełnomocnika i ADO.
4.Za organizację terminowego przeprowadzenia przeglądów oraz ich prawidłowy przebieg odpowiada ADO/Pełnomocnik.

§ 35

1.Przeglądy programów i narzędzi programowanych przeprowadzany jest w przypadku zmiany:
1) oprogramowania serwera plików,

2) wersji oprogramowania stanowiska komputerowego użytkownika systemu,
3) systemu operacyjnego serwera plików,
4) systemu operacyjnego stanowiska komputerowego użytkownika systemu,
5) w projekcie systemu spowodowanej koniecznością naprawy, konserwacji lub modyfikacji systemu.

2. Przed wprowadzeniem zmiany w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowanej bazie danych. Sprawdzenie powinno obejmować:
   1) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów urządzeń użytkownika);
   2) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty);
   3) poprawność funkcjonowania systemu symulując działania grupy użytkowników wykonując następujące operacje: - wprowadzanie danych osobowych,
      - edytowanie danych osobowych, - wyszukiwanie danych osobowych,
      - wydruk danych osobowych.
3. Przegląd przeprowadza ADO/Pełnomocnik.

§ 36

1. W przypadku zdalnego dostępu do komputera (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez ADO/Pełnomocnika lub osobę przejmującą pulpit komputera, której zlecone zostały stosowane działania.
2. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają kontroli i sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:
   1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem,
   2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie ADO),
   3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu), 4) zakres prac serwisowych i ich wynik,
   5) czas przeprowadzania prac serwisowych.

§ 37

Przeglądu i konserwacji systemu dokonuje się w regularnych odstępach czasu.

Przepisy końcowe Części II.

§ 38

Zmiany Instrukcji wprowadza ADO lub Pełnomocnik za zgodą ADO.

Załącznik 1

Wzór upoważnienia z oświadczeniem

………………………………… …………., dnia…………………………

(pieczęć Administratora Danych)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 32 ust 4 Rozporządzenia 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, zwane dalej RODO, upoważniam

P a n i ą / P a n a : … .
……………………………………………………

Zatrudnioną/-ego na stanowisku/ współpracującego w zakresie:
……………………………………………………………….……………………..

Do przetwarzania danych osobowych w związku z wykonywaniem obowiązków związanych z zatrudnieniem lub w zakresie wynikającym z zajmowanego stanowiska pracy.

Upoważnienie udzielane jest na czas trwania zatrudnienia (do odwołania).

……………………………………………………………..……………………….

podpis osoby reprezentującej Administratora Danych

OŚWIADCZENIE

Niniejszym zobowiązuję się do zachowania poufności danych osobowych przetwarzanych w Żłobek uRodzinki, uRodzinki Sp. z o.o. z siedzibą w Ćmiłowie 53, 20-388 Lublin, tj. zarówno w charakterze administratora, jak i podmiotu przetwarzającego - nieujawniania ich osobom nieupoważnionym i zachowania w tajemnicy informacji o sposobach, środkach i technikach zabezpieczeń tych danych.

Jednocześnie zobowiązuję się do przetwarzania danych osobowych, do których mam lub będę miał(a) dostęp z tytułu wykonywania swoich zadań i obowiązków służbowych /pracowniczych, wyłącznie na polecenie administratora (ADO).

Potwierdzam przy tym, że zapoznałem/-am się z:

- definicją danych osobowych w rozumieniu art. 4 pkt 1 Rozporządzenia 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, tj.: „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”) -możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, m.in. na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających np. fizyczną, czy społeczną tożsamość osoby fizycznej;

- Polityką bezpieczeństwa przetwarzania danych i zobowiązuję się do jej przestrzegania.

Jednocześnie jestem świadomy/a, że osoby upoważnione do przetwarzania danych zobowiązane są zachować w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia, także po ustaniu stosunku pracy lub po upływie ważności upoważnienia. Ponadto podlegają odpowiedzialności karnej wynikającej, m.in. z art. 266 i n. kodeksu karnego.

Zobowiązuje się do nierozpowszechniania i niewykorzystywania informacji zdobytych w trakcie wykonywania obowiązków pracowniczych/ wynikających z zatrudnienia, także po jego ustaniu. Z chwilą ustania zatrudnienia zobowiązuje się do niezwłocznego zwrócenia pracodawcy wszelkich dokumentów oraz innych materiałów zawierających dane osobowe, do których przetwarzania nie posiadam prawa.

Przyjmuję do wiadomości i akceptuję, iż dane osobowe stanowią element tajemnicy przedsiębiorstwa, a postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie podstawowych obowiązków kontraktowych lub obowiązków pracowniczych w rozumieniu przepisów Kodeksu Pracy oraz, że Pracodawca/Zatrudniający, jako strona poszkodowana ma prawo do dochodzenia na zasadach ogólnych odszkodowania odpowiadającego wysokości poniesionej szkody lub innej odpowiedzialności na zasadach wynikających z dalszych przepisów prawa.

.....

(data, podpis pracownika)

Zgoda Pracownika

..... ……., dnia.....
(nazwisko i imię)
.....
(stanowisko Pracownika)

Informacja i oświadczenie w sprawie danych osobowych

W związku z zatrudnieniem u Pracodawcy, niniejszym oświadczam, że dobrowolnie przekazuję dane osobowe -część lub wszystkie wymienione poniżej.

Dane osobowe: imię (imiona) i nazwisko, data urodzenia, adres do korespondencji, nazwisko rodowe, obywatelstwo i płeć, tytuł ubezpieczenia, stopień niepełnosprawności, posiadanie ustalonego prawa do emerytury lub renty, adres zameldowania na stałe miejsce pobytu, adres poczty elektronicznej, numer telefonu, wykształcenie, historia zatrudnienia, dodatkowe umiejętności i uprawnienia niezbędne do wykonywania pracy danego rodzaju w tym znajomość języków obcych, odbyte kursy i szkolenia zawodowe, adres zamieszkania, numer PESEL, rodzaj i numer dokumentu potwierdzającego tożsamość, w przypadku braku numeru PESEL, numer NIP w przypadkach określonych w art. 33 ust. 2 ustawy o systemie ubezpieczeń społecznych, dane osobowe dzieci pracownika oraz dane osobowe innych członków rodziny pracownika oraz dane osobowe osób pozostających z pracownikiem we wspólnym gospodarstwie domowym lub osób bliskich takie jak: imię i nazwisko, data urodzenia, stopień pokrewieństwa, adres zamieszkania oraz inne dane niezbędne do stwierdzenia lub korzystania z uprawnień przewidzianych w ustawie o zakładowym funduszu świadczeń socjalnych, numer telefonu osoby, którą należy powiadomić o wypadku lub innym nieszczęśliwym zdarzeniu z udziałem pracownika, dane dotyczące aktualnego zatrudnienia w tym: rodzaj umowy o pracę, stanowisko pracy, miejsce wykonywania pracy, wymiar etatu, zakres obowiązków, wysokość wynagrodzenia za pracę oraz inne składniki wynagrodzenia, lista obecności i informacje tam zawarte (także dotyczące nieobecności i jej przyczyn dla potrzeb zapewnienia właściwej organizacji pracy), informacje o zasiłkach, wynagrodzeniu chorobowym, o odprawach, rekompensatach oraz innych świadczeniach pieniężnych i niepieniężnych ze stosunku pracy, dane związane z kasą zapomogowo-pożyczkową i korzystaniem z jej świadczeń, dane dotyczące zajęcia wynagrodzenia przez organy egzekucyjne, dane dotyczące potrąceń z wynagrodzenia, dane dotyczące korzystania z uprawnień rodzicielskich i urlopowych, dane dotyczące korzystania z uprawnień urlopowych, płatnych lub nieodpłatnych zwolnień z pracy przysługujących na podstawie odrębnych od kodeksu pracy przepisów prawa, inne dane dotyczące przebiegu zatrudnienia, w tym dane o odbytych szkoleniach z zakresu BHP, wykonanych badaniach z zakresu medycyny pracy, dane dotyczące stopnia niepełnosprawności, dane dotyczące podnoszenia kwalifikacji przez pracowników w czasie trwania stosunku pracy, dane dotyczące kar porządkowych przez okres ustalony przepisami prawa pracy, informacje o zmianie i rozwiązaniu stosunku pracy, informacje dotyczące numeru rachunku bankowego oraz banku prowadzącego rachunek pracownika, dane dotyczące samochodów prywatnych pracowników wykorzystywanych do celów służbowych, w zakresie niezbędnym do prowadzenia przewidzianej prawem dokumentacji, w tym ewidencji przebiegu pojazdu, dane dotyczące udziału w pracowniczych programach emerytalnych, dane ubezpieczeniowe zawarte w imiennych raportach miesięcznych, dane zawarte w zaświadczeniach lekarskich o czasowej niezdolności do pracy, dane dotyczące korzystania przez pracowników z usług niezwiązanych bezpośrednio ze stosunkiem pracy świadczonych na rzecz pracowników przez Pracodawcę lub inne podmioty, w tym rodzaj oraz adres placówki świadczącej usługi kontraktowanej (prywatnej) opieki zdrowotnej, nadto informacje zawarte w dokumentach przedkładanych Pracodawcy oraz zdjęcie i wizerunek w związku z funkcjonowaniem monitoringu wizyjnego miejsc (po jego wprowadzeniu) oraz dla promowania wizerunku Pracodawcy.

Jednocześnie oświadczam, że wyrażam zgodę na przetwarzanie danych osobowych przekazanych Pracodawcy, w tym też na przyszłość, związanych z zatrudnieniem,

wykonywaniem obowiązków służbowych/pracowniczych, realizacją interesu Pracodawcy i o niego dbałością oraz interesu Pracownika. W przypadku przekazywania danych nie dotyczących mojej osoby - potwierdzam, iż każdorazowo posiadam do tego umocowanie, a osoby których dane dotyczą znają cel, podmioty realizujące cele i uprawnienia z tego płynące, tak w związku z realizacją obowiązku prawnego, jak i interesie tych osób.

Dane osobowe pozyskane od Pracownika, przetwarzane są i będą w celu i zakresie niezbędnie wymaganym przepisami prawa lub realizacją zadań Pracodawcy, i przekazywane podmiotom/organom, w związku z dyspozycją przepisów prawa i w związku z prowadzoną działalnością oraz umowami i innymi stosunkami prawnymi przy tym powstającymi.

Przechowywanie oraz przetwarzanie danych odbywa się w celu i w okresie trwania zatrudnienia, w celu i w okresie wykonywania związanych z tym obowiązków wynikających z przepisów prawa, interesie Pracodawcy lub w interesie Pracownika. Pracodawca jest administratorem danych osobowych. Pracownikowi przysługuje prawo dostępu do treści udostępnionych danych, ich poprawiania, przenoszenia oraz zgłoszenia skargi do organu nadzorczego. Przekazanie danych osobowych jest dobrowolne, ale konieczne dla zawarcia i wykonywania Umowy, w interesie Pracownika.

.....
Data i podpis

przykładowa ewidencja osób upoważnionych

LP.	Imię i nazwisko	Login / Identyfikator	System informatyczny - zakres	Zakres upoważnienia (zasoby nieinformatyczne) - zakres	Data nadania	Data ustania	Uwagi

Załącznik nr 2

Rejestr czynności/ kategorii przetwarzania

a) nazwa oraz dane kontaktowe ADO: uRodzinki Sp. z o.o. z siedzibą w Ćmiłowie 53, 20-388 Lublin

b) cele przetwarzania (A- jako administrator; P- jako podmiot przetwarzający):

1) A: opieka na wychowankami, umowy o pracę, umowy pozyskania usług i dostaw ze strony podmiotów trzecich, organizacja usług, świadczenie usług medycznych - czynności leczniczych - w związku z przedmiotem naszej działalności oraz dla działania w celu poszukiwania i pozyskiwanie (rozpoczęcia współpracy) podmiotów świadczących na naszą rzecz usługi oraz realizujących dostawy oraz klientów, w tym m.in. organizowanie i logistyka realizacji zamówień/zleceń, zgłoszeń oraz reklamacji, promocji i marketingu;
2) P- realizacja umów na rzecz klientów, zakres określa umowa oraz przepisy prawa.

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych:

1) Rodzice dzieci żłobkowych, klienci, kontrahenci, współpracownicy, w zakresie: imienia i nazwiska, firmy, adresu, nr-y: NIP, REGON, PESEL, adres e-mail, nr telefonu, danych rozliczeniowych - podstawa ustalania wynagrodzenia, historia współpracy, adresy dostaw, inne wynikające z przepisów prawa;
2) Pracownicy, w zakresie: jak we wzorze informacji dla Pracownika, zgodnie z zapisami załączników Polityki bezpieczeństwa;
3) kandydaci do pracy - w zakresie: sformułowane wymogi oraz treść dokumentów i informacji przedkładanych wraz z aplikacją;
4) zainteresowani współpracą, potencjalni współpracownicy - w zakresie: imię i nazwisko, firma, adres, NIP, nr telefonu, adres e-mail, dane o prowadzonej działalności oraz dane wynikające z obowiązków wobec urzędów, organów, instytucji (np. wobec ZUS);
5) dane przetwarzane na rzecz klientów - zgodnie z umowami, w ich zakresie, zgodnie z przepisami prawa.

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione: A.

1) organy i podmioty - ze względu na obowiązki wynikające z przepisów prawa;
2) podmioty świadczące usługi i realizujące dostawy na rzecz Administratora, wspierające jego działalność lub udostępniające kompetencje.

P. - zgodnie z uwarunkowaniami poszczególnych umów, w zakresie związanym z koniecznością lub poleceniem/zgodą klienta pozyskania kompetencji/usług podmiotu trzeciego.

e) planowane terminy usunięcia poszczególnych kategorii danych:

1) po okresie ustania współpracy, wykonania i rozliczenia umów oraz wypełnienia obowiązków prawnych po stronie Administratora;

f) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa:

Zgodnie z treścią Polityki bezpieczeństwa, ADO korzysta z odpowiednio dobranych rozwiązań i narzędzi:

1) zabezpieczenia technicznego systemu - właściwości konfiguracji, rodzaju i specyfiki wykorzystywanych programów;
2) sposobu zorganizowania działalności - pragmatyki, sposób wypełniania obowiązków, szkolenia;
3) dozór fizyczny;
4) alarm (w przypadku wprowadzenia).

Załącznik 3

Ocena ryzyka dla ochrony danych /i szacowanie skutków

I. Lista potencjalnych zagrożeń w przetwarzaniu danych osobowych.

ATAKI ZEWNĘTRZNE	
	Ataki socjotechniczne
Zagrożenie	**Opis**
Phishing	Mail z prośbą o zalogowanie się do „podróbki” strony, np. bankowe i w rezultacie przejęcie hasła.
cybersquatting	Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym” adresie www

wyłudzanie informacji	▪ maile od „przełożonych” np. z dyspozycją wykonania przelewu, ▪ faxy, w których intruz podszywa się pod dostawcę i informuje o zmianie numeru konta bankowego, ▪ maile lub rozmowy tel., w których intruz podaje się np. za pracownika firmy dostarczającej oprogramowanie i prosi o hasło w celu „przetestowania uprawnień”
nakłanianie do wykonania czynności	Maile, które zachęcają lub „zmuszają” do otwarcia załączników
ataki telefoniczne	▪ intruz przedstawia się jako pracownik dostawcy łącza naprawiający usterkę i prosi o uruchomienie określonej strony internetowej, ▪ intruz przedstawia się jako inżynier lub programista dostawcy oprogramowania w celu np. przesłania „aktualizacji” lub prosi o udostępnienie pulpitu

Złośliwe oprogramowanie	▪ oprogramowanie szyfrujące pliki, ▪ oprogramowanie przechwytujące dane, ▪ trojany,
	Ataki na infrastrukturę
Zagrożenie	**Opis**
łamanie i pozyskiwanie haseł	▪ łamanie haseł, przechowywanie haseł na karteczkach, włamania do urządzeń ▪ nieaktualizowanych, ▪ ▪ odgadywanie zbyt słabych, najpopularniejszych haseł np. 123456789, ▪ stosowanie domyślnych haseł producenta i brak jego zamiany po pierwszym logowaniu; ▪ posiłkowanie się jednym hasłem do wielu systemów, programów, ▪ niezmieniane hasła, nawet po incydencie,

	▪ włamania do urządzeń nieodpowiednio skonfigurowanych, ▪ włamania z użyciem niezabezpieczonych interfejsów lokalnych, włamania za pośrednictwem niepotrzebnych usług
Ataki na sprzęt	▪ włamania do urządzeń nieodpowiednio skonfigurowanych, ▪ włamania z użyciem niezabezpieczonych interfejsów lokalnych, ▪ włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze).
Ataki na oprogramowanie	▪ wykorzystanie znanych atakującemu dziur w nieaktualizowanym oprogramowaniu, ▪ włamania z wykorzystaniem domyślnych haseł (łatwe hasła), ▪ włamania z wykorzystaniem najczęstszych błędów, ▪ włamania z wykorzystaniem API (interfejsów programistycznych)
Skanowanie sieci i usług	Atakujący poznaje wersję systemu operacyjnego lub wersję serwera www, a przez to potem może dobrać skuteczny atak
Nielegalne wpięcie się do sieci (wifi, telefon, internet)	Łatwo dostępne gniazdka sieciowe, gdzie atakujący może się podłączyć np. z własnym urządzeniem i za jego pomocą przeglądać zasoby sieci (możliwość podpięcia się np. pod drukarkę na korytarzu lub do in.gniazdka)

Eskalacja uprawnień	▪ zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych, ▪ przejęcie uprawnień użytkownika zaawansowanego, ▪ przejęcie uprawnień administratora, ▪ przejęcie uprawnień systemowych, ▪ przejęcie certyfikatów elektronicznych,
Ataki tzw. “Man in the middle”	Przejęcie komputera w placówce w celu włamania do sieci (w rezultacie możliwość przejęcia haseł)
	Zagrożenia dla sprzętu

Zagrożenie	Opis
Włamanie do obiektów	Może skutkować zainstalowaniem nieautoryzowanych urządzeń
Kradzież / zniszczenie sprzętu	kradzież komputerów w organizacji i laptopów poza nią, uszkodzenie sprzętu na skutek przepięcia, czy upadku,
Pożar / eksplozja	pożar, wybuch gazó
Zalanie	np. powódź, pęknięta rura kanalizacyjna, zalanie kawą,
Przegrzanie	wysoka temperatura urządzeń lub w serwerowni,
Awaria zasilania	skoki napięcia / przerwy w dostawie,
Awaria sprzętu	awaria dysków, modułów, płyty głównej, sterowników, routerów,
Starzenie się nośników danych	Zbyt długie eksploatowanie nośników danych może powodować ryzyko utraty zawartości,

ZAGROŻENIA DANYCH

Zagrożenie	Opis
Nieuprawniony dostęp	nadanie zbyt wysokich uprawnień użytkownikom lub brak kontroli nad dostępem do plików, baz, komputerów,
Kradzież tożsamości	przejęcie poczty, pozyskanie danych z dowodu osobistego i w rezultacie np. założenie firmy „słupa”, wyłudzenie kredytu, zakupy na cudze konto,
Nieuprawniona modyfikacja / usunięcie	▪ niezamierzona lub w efekcie pomyłki, ▪ sfałszowanie danych przez osoby z wewnątrz lub zewnątrz placówki.
Nieuprawnione kopiowanie danych	▪ kopiowanie danych z katalogów, dysków, baz, programów, kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą

Kradzież danych lub nośników	Na zewnątrz i wewnątrz placówki
Utrata / kradzież danych dostępowych	haseł, kluczy, certyfikatów
Błąd / awaria oprogramowania	uszkodzenie bazy danych, programu kadrowo-płacowego
Brak / błędy w wykonywaniu kopii bezpieczeństwa	doraźne lub zbyt rzadkie wykonywanie kopii, błędy podczas procesu wykonywania kopii, kopie dostępne w sieci lub archiwum bez zabezpieczeń,
Udostępnianie danych osobom nieupoważnionym	upublicznienie danych w przestrzeni publicznej, dostęp przez internet, przesłanie lub wydawanie informacji osobie nieupoważnionej, wyrzucanie na śmietnik,
Nieprawidłowe / brak procedur niszczenia nośników z danymi	wyrzucenie uszkodzonych nośników bez ich zniszczenia, wyrzucenie niezniszczonych pendrive, DVD, CD
Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	Naprawa sprzętu z nośnikami w serwisie bez standardu bezpiecznej naprawy i bez umowy bezpieczeństwa.
Korzystanie z nielicencjonowanego/ nielegalnego oprogramowania	Wykorzystywanie nielegalnych, kradzionych, nielicencjonowanych aplikacji i oprogramowania.

BŁĘDY LUDZKIE	
Zagrożenie	**Opis**

Nieprzestrzeganie procedur	Świadome naruszenie pisemnych lub ustnych procedur, np. niewylogowywanie się z systemu, przekazywanie haseł koledze, pozostawienie haseł na karteczce przy komputerze,
Pomyłki administratorów, użytkowników	Pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia
Brak świadomości / wiedzy	braki wiedzy, nieszkolony personel, brak procedury niszczenia nośników danych,
Błędy projektowe / konfiguracyjne	Błędy programistów prowadzące do niewłaściwego przetwarzania danych, niezabezpieczenie danych w bazie www przed indeksacją.

ZAGROŻENIA CIĄGŁOŚCI DZIAŁANIA	
Zagrożenie	**Opis**
Brak aktualnej dokumentacji	Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania utrudnia przywracanie środowiska i zarządzanie nim, gdy np. odejdzie pracownik IT/ dostawca usług
Nieprawidłowe / brak umowy o współpracy	Brak zapisów przenoszących odpowiedzialność na zleceniobiorcę lub podmiot przetwarzający dane,
Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	Niewłaściwie skonstruowane umowy, nieprzedłużane umowy, zbyt długi czas reakcji serwisu na awarie
Upadek firmy współpracującej np. dostawcy oprogramowania /serwera	Ryzyko braku zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji lub oprogramowania

Awaria łączy telekomunikacyjnych	Awaria jest krytyczna w przypadku usług chmurowych

II.

Wobec przeprowadzonych analiz i ustalenia, iż w związku z przetwarzaniem danych nie występuje wysokie ryzyko naruszenia praw i wolności osób, których dane są przetwarzane, a dodatkowo prawdopodobieństwo wystąpienia tego ryzyka - wobec wdrożonych procedur i środków zabezpieczających, a przede wszystkim wobec ograniczonego zakresu danych osobowych podlegających przetwarzaniu i wobec charakteru czynności przetwarzania dla prowadzonej działalności i ograniczenia wykorzystywania systemów teleinformatycznych oraz zakresu danych w nich przetwarzanych - nie jest szczególnie istotne, co pozwala na odstąpienie od przeprowadzania oceny skutków dla ochrony danych. Powyższe wynika bezpośrednio z faktu:

1) operacje przetwarzania wynikają z realizacji zadań placówki, zadań jako pracodawcy oraz prowadzeniu działalności w ograniczonych ramach organizacyjnych i terytorialnych, a dodatkowo zawsze w związku z obowiązkiem zachowywania tajemnic służbowych;
2) realizowane operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów prowadzonej działalności;
3) środki bezpieczeństwa, tak organizacyjne, jak i techniczne opisane w Polityce bezpieczeństwa, są dostateczne do skali ryzyka prowadzonej działalności.

Uwaga:

Z informacji podawanych przez organ nadzorczy może płynąć nakaz rozszerzenia powyższego opracowania, w tym w zakresie innych rodzajów operacji.

Załącznik 4

Procedura weryfikacji naruszeń

Po otrzymaniu zawiadomienia o naruszeniu bezpieczeństwa systemu przetwarzania danych osobowych Administrator lub Pełnomocnik powinien niezwłocznie:

I.

1) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia i osoby odpowiedzialnej za naruszenie:

- zapisać wszelkie informacje związane z danym zdarzeniem,
- wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je data i podpisem,

3) określić dokładnie rodzaj, sposób oraz rozmiar naruszenia zabezpieczenia systemu teleinformatycznego;
4) podjąć działania zabezpieczające system przed ponownym naruszeniem:
   - fizyczne odłączenie urządzeń i segmentów sieci, które mogą uniemożliwić dostęp do bazy danych osobie nieupoważnionej,
   - wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
   - zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.
5) dokonać wstępnej analizy stanu systemu teleinformatycznego, w celu potwierdzenie lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie, tj. sprawdzenie :
   - stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,
   - zawartości zbioru danych osobowych,
   - sposobu działania programów,
   - jakości komunikacji w sieci komputerowej,
   - możliwości obecności wirusów komputerowych.
6) przeprowadzić szczegółową analizę stanu systemu teleinformatycznego obejmującą:
   - rodzaj zaistniałego zdarzenia,
   - metody i zakresu dostępu do danych osoby nieupoważnionej, - skali zniszczeń.
7) przywrócić prawidłowy stan działania systemu (w przypadku kiedy nastąpiło uszkodzenie bazy danych należy odtworzyć ostatnią kopię awaryjną, z zachowaniem wszelkich środków ostrożności mając na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę nieupoważnioną),
8) sporządzić notatkę służbową z przebiegu zdarzenia, która obejmuje:
   - dane osoby stwierdzającej naruszenie ochrony,
   - datę, godzinę i miejsce naruszenia ochrony,
   - rodzaj naruszenia ochrony,
   - czas powiadomienia o zdarzeniu,
   - opis podjętych czynności, - wnioski do realizacji.

II.

Jeżeli przyczyną zdarzenia było:

1) popełnienie błędu przez pracownika przy przetwarzaniu danych osobowych w systemie informatycznym - należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych,
2) uaktywnienie wirusa - należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe,
3) zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, - należy rozważyć wyciągnięcie konsekwencji prawnych,
4) włamanie w celu pozyskania bazy danych osobowych - należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia ochrony bazy danych,
5) korzystanie z złych pod względem technicznym urządzeń bądź nieprawidłowo działającego programu - należ wówczas zalecić wykonanie czynności serwisowoprogramowych.

III.

W przypadku kradzieży, należy niezwłocznie powiadomić o tym fakcie Policję.

IV.

W przypadku naruszenia zabezpieczenia systemu informatycznego przed przystąpieniem do dalszej pracy, należy dokonać zmiany haseł i identyfikatorów lub zmiany innych zabezpieczeń.

V.

Wyrazić zgodę /lub wydać inne dyspozycje - na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowania przetwarzania danych lub modyfikacji tych procesów.

Załącznik 5

WZÓR ZGŁOSZENIA INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

…….

Miejscowość, data

Prezes Urzędu Ochrony Danych Osobowych

……

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora Danych Osobowych	
Miejsce i dzień naruszenia	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Opis charakteru naruszenia ochrony danych	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

……..

Podpis osoby uprawnionej do reprezentowania

Administratora Danych Osobowych