Zarządzenie Nr 34/DN/ 2013

Dyrektora Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli
z dnia 28 sierpnia 2013 r.
w sprawie aktualizacji dokumentacji przetwarzania danych osobowych w LODR w Końskowoli

Na podstawie § 17 Regulaminu Organizacyjnego LODR w Końskowoli oraz art. 3 ust 1 i art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) w związku z § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) – zarządzam co następuje:

§ 1

Wprowadzam dokumentację przetwarzania danych osobowych w Lubelskim Ośrodku Doradztwa Rolniczego w Końskowoli, na którą składają się:

1) Polityka bezpieczeństwa informacji Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli, stanowiąca załącznik nr 1 do niniejszego zarządzenia,
2) Instrukcja ochrony danych osobowych przetwarzanych w systemie informatycznym Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli, stanowiąca załącznik nr 2 do niniejszego zarządzenia.

§ 2

Aktualizacja wykazu zbiorów danych prowadzonych w LODR w Końskowoli, opisu struktury tych zbiorów oraz wykazu budynków i pomieszczeń, tworzących obszar przetwarzania danych osobowych, stanowiących załączniki do Polityki bezpieczeństwa informacji LODR w Końskowoli, nie wymaga każdorazowo zmiany zarządzenia.

§ 3

Zobowiązuję Kierowników komórek organizacyjnych do zapoznania z wyżej wymienionymi dokumentami wszystkie osoby upoważnione do przetwarzania danych osobowych w LODR.

§ 4

Nadzór i kontrolę nad prawidłowym wykonaniem zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§ 5

Traci moc dotychczas obowiązujące Zarządzenie Nr 23/DN/2000 z dnia 25 lipca 2000 r.

§ 6

Zarządzenie wchodzi w życie z dniem 28 sierpień 2013 r.

DYREKTOR
mgr Antoni Skrabucha

Polityka bezpieczeństwa informacji Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli

I. Postanowienia ogólne

1. Wstęp

Wdrożenie Polityki bezpieczeństwa informacji w Lubelskim Ośrodku Doradztwa Rolniczego w Końskowoli ma na celu uzyskanie dla przetwarzania danych osobowych optymalnego poziomu zabezpieczenia oraz zgodności z wymogami obowiązujących przepisów prawnych.

Utrzymanie bezpieczeństwa przetwarzania danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i rozliczalności na odpowiednim poziomie.

Poufność danych – oznacza, że dane nie są udostępniane nieupoważnionym podmiotom.

Integralność danych – oznacza, że dane osobowe nie zostały zmienione, dodane lub usunięte w sposób nieautoryzowany.

Rozliczalność danych – oznacza, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Dokumentem związanym z Polityką jest Instrukcja ochrony danych osobowych przetwarzanych w systemie informatycznym Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli (dalej zwana Instrukcją) oraz procedura P-SZJ/005 Nadzór nad sprzętem informatycznym. Stanowią one uszczegółowienie niektórych postanowień Polityki w zakresie przetwarzania danych osobowych w systemie informatycznym.

2. Znaczenie bezpieczeństwa danych osobowych i odpowiedzialność za ich ochronę

Właściwe zabezpieczenie danych, jest istotne z uwagi na odpowiedzialność w stosunku do osób, które powierzają dane LODR w Końskowoli. Chęć profesjonalnego działania przekłada się także na obowiązek zastosowania środków bezpieczeństwa odpowiednich do istniejących zagrożeń.

Ustawa o ochronie danych osobowych określa surowe sankcje karne, z pozbawieniem wolności włącznie, za naruszenie obowiązków ochrony danych osobowych, również w przypadku działań nieumyślnych.

Za ochronę danych osobowych odpowiada Dyrektor LODR, który podejmuje decyzje o celach i środkach przetwarzania danych. Każdy pracownik, w codziennej pracy, powinien przestrzegać przepisów prawa i procedur przetwarzania danych osobowych, a w zakresie niesprecyzowanym w Polityce i Instrukcji stosować odpowiednie podejście tak, aby zapewnić bezpieczeństwo danych osobowych. Za stosowanie w LODR środków zabezpieczających dane osobowe w szczególny sposób odpowiadają osoby pełniące funkcje kierownicze.

3. Zagrożenia i poziom bezpieczeństwa przetwarzania danych osobowych

Dane osobowe podlegają zagrożeniom umyślnego i nieumyślnego udostępnienia osobom niepowołanym oraz uszkodzeniu lub utracie, a urządzenia służące do przetwarzania danych osobowych połączone są z siecią publiczną. W związku z powyższym stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych, zgodnie z Rozporządzeniem Ministra Spraw

Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Oprócz środków związanych z zabezpieczeniem danych należy zwracać uwagę na adekwatność zbieranych danych, w stosunku do celów przetwarzania. Należy ograniczać ilość i zakres zbieranych danych do tych niezbędnych.

4. Zakres stosowania Polityki bezpieczeństwa informacji

Regulacje zawarte w Polityce mają zastosowanie do:

a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe;

b) dokumentów zawierających dane osobowe przetwarzanych w formie papierowej;

c) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane dane osobowe;

d) wszystkich pracowników, stażystów oraz innych osób mających dostęp do danych osobowych;

e) wszystkich danych osobowych przetwarzanych w LODR, będących jego własnością lub w inny sposób podlegających jego ochronie.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

5. Definicje

Ilekroć w Polityce jest mowa o:

przetwarzaniu danych - rozumie się przez to 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;

systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

administratorze danych – rozumie się przez to Dyrektora LODR;

osobie upoważnionej do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Dyrektora LODR na piśmie;

użytkowniku – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;

identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.

II. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Aktualny wykaz budynków i pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa Załącznik nr 1.

III. Wykaz zbiorów danych osobowych oraz programów służących do ich przetwarzania

Aktualny wykaz zbiorów danych osobowych oraz programów służących do ich przetwarzania określa Załącznik nr 2.

IV. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązań między nimi

Aktualny opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w Załączniku 3 do niniejszego dokumentu.

V. Sposób przepływu danych pomiędzy systemami

Dane osobowe pracowników LODR ze zbioru kadrowo-płacowego są udostępniane organom prowadzącym kontrolę, w tym zwłaszcza Państwowej Inspekcji Pracy i sądom powszechnym w związku z prowadzonym postępowaniem, urzędom skarbowym oraz ZUS-owi za pomocą programu Płatnik. Wykorzystując system bankowości elektronicznej VideoTel, tworzy się przelewy wynagrodzeń.

Dane odbiorców usług doradczych i szkoleniowych wprowadzane są do Rejestru usług doradczych LODR znajdującego się w systemie elektronicznej Sprawozdawczości pracy doradczej.

Dane osób prowadzących rachunkowość rolniczą w ramach zunifikowanego systemu rachunkowości gospodarstw rolnych - Polski FADN przesyłane są do Instytutu Ekonomiki Rolnictwa i Gospodarki Żywnościowej - Państwowy Instytut Badawczy zgodnie z europejskim systemem zbierania danych rachunkowych z gospodarstw rolnych.

Pozostałe systemy, w których przetwarza się dane osobowe są rozproszone i nie są ze sobą połączone, co uniemożliwia przepływ danych pomiędzy nimi.

VI. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Zastosowane środki

Środki ochrony fizycznej:

a) urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zamykanych na klucz;
b) dostęp do pomieszczenia, w którym znajdują się urządzenia serwerowe ma tylko Administrator Systemu Informatycznego.

Środki sprzętowe, informatyczne, telekomunikacyjne:

a) stosuje się niszczarki dokumentów;

b) urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których są przetwarzane dane osobowe podłączone są do lokalnych awaryjnych zasilaczy ups, zabezpieczających przed skokami napięcia i zanikiem zasilania;
c) sieć lokalna skonfigurowana jest w topoli gwiazdy;
d) sieć lokalna podłączona jest do internetu poprzez router spełniający jednocześnie funkcję zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną.

Środki ochrony w ramach oprogramowania urządzeń teletransmisji:
a) na komputerach użytkowników systemu działa program antywirusowy;
b) na komputerach użytkowników systemu działa programowy firewall;
c) dostęp do serwera zawierającego dane osobowe zabezpieczony jest hasłem.

Środki ochrony w ramach oprogramowania systemu:
a) dostęp do baz danych osobowych zastrzeżony jest wyłącznie dla uprawnionych pracowników;
b) system informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu odrębnie dla każdego pracownika;
c) zastosowano działający w tle program antywirusowy na komputerach użytkowników.

Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:
a) zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji;
b) dla każdego użytkownika systemu wyznaczony jest odrębny identyfikator.

Środki ochrony w ramach systemu użytkowego:
a) komputer, z którego możliwy jest dostęp do danych osobowych jest zabezpieczony hasłem uruchomieniowym;
b) zastosowano wygaszenie ekranu.

Środki organizacyjne:
a) wyznaczono administratora bezpieczeństwa informacji;
b) wyznaczono administratora systemu informatycznego;
c) do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane są osoby na podstawie upoważnienia;
d) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania ich w tajemnicy;
e) administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego;
f) przeprowadzane są szkolenia dla osób zatrudnionych przy przetwarzaniu danych osobowych w zakresie obowiązujących aktów prawnych oraz wewnętrznych przepisów i procedur.

2. Mechanizmy kontroli dostępu do danych osobowych w systemach informatycznych

Wszyscy użytkownicy przetwarzający dane osobowe w systemach informatycznych powinni posiadać indywidualne identyfikatory z przydzielonym zakresem uprawnień oraz hasło.

Dostęp do danych osobowych w systemach informatycznych i ich przetwarzanie jest dopuszczalne wyłącznie na indywidualnym profilu użytkownika po wprowadzeniu własnego identyfikatora i hasła. Nie wolno udostępniać profilu użytkownika oraz hasła innym osobom.

Ponadto dostęp do programów, w których przetwarzane są dane osobowe, powinien być możliwy tylko po wprowadzeniu indywidualnego identyfikatora i hasła. Nie dotyczy to programów MS OFFICE i podobnych, służących wyłącznie do edycji tekstu i udostępniana go na piśmie.

Instrukcja określa procedurę przydziału identyfikatora i uprawnień w systemach informatycznych.

3. Sposób postępowania z komputerami przenośnymi i nośnikami informacji

Ze względu na swój charakter, przenośne komputery i nośniki informacji są dużo bardziej podatne na uszkodzenia, zagubienie i utratę niż innego rodzaju sprzęt informatyczny. Dlatego też należy zachować ostrożność podczas ich użytkowania, przechowywania i przenoszenia.

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe określonym Załącznikiem nr 1.

Zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

4. Kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Kopie bezpieczeństwa danych osobowych powinny być tworzone w celu zabezpieczenia danych przed przypadkową lub nieuprawnioną zmianą bądź skasowaniem.

Tworzeniu kopii zapasowych podlegają: zbiory danych osobowych, programy i narzędzia programowe służące do przetwarzania danych osobowych oraz inne zbiory danych i programy zgodnie z Instrukcją. Dotyczy to zarówno komputerów stacjonarnych i przenośnych, jak i serwerów.

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli
Centrala, ul. Pożowska 8, 24-130 Końskowola Pomieszczenia: - piwnica - archiwum zakładowe; - parter, numery pokojów: 1, 2, 4-9; - I piętro, numery pokojów: 11-14,16,18; - II piętro, numery pokojów: 21-30.
Budynek Działu Przedsiębiorczości, Wiejskiego Gospodarstwa Domowego i Agroturystyki, ul. Pożowska 8, 24-130 Końskowola
Centrum Innowacyjno-Szkoleniowe (recepcja), ul. Pożowska 8, 24-130 Końskowola
Zespoły Doradztwa Rolniczego
ZDR w Bełżycach, ul. Fabryczna 2 b, 24-200 Bełżyce
ZDR w Białej Podlaskiej z/s w Grabanowie, Grabanów, 21-500 Biała Podlaska
ZDR w Biłgoraju, ul. M. Konopnickiej 7, 23-400 Biłgoraj
ZDR w Bychawie, ul. A. Mickiewicza 15, 23-100 Bychawa
ZDR w Chełmie, Pl. Niepodległości 1 (parter, skrzydło E, pokój 80), 22-100 Chełm
ZDR w Elizówce, Elizówka 65 E (pokoje 105, 106), 21-003 Ciecierzyn
ZDR w Hrubieszowie, ul. 3-go Maja 37, 22-500 Hrubieszów
ZDR w Janowie Lubelskim, ul. Bialska 11, 23-300 Janów Lubelski
ZDR w Końskowoli, ul. Pożowska 8, 24-130 Końskowola
ZDR w Krasnymstawie, ul. Sobieskiego 3, (budynek starostwa, III piętro, pokoje 312-315), 22-300 Krasnystaw
ZDR w Kraśniku, ul. Niepodległości 20, 23-204 Kraśnik
ZDR w Lubartowie, ul. Szaniawskiego 64, 21-100 Lubartów
ZDR w Łęcznej, ul. Jana Pawła II 95, 21-010 Łęczna
ZDR w Łukowie, ul. Przemysłowa 15, 21-400 Łuków
ZDR w Opolu Lubelskim, ul. Przemysłowa 16, 24-300 Opole Lubelskie
ZDR w Parczewie, ul. Lubartowska 4, 21-200 Parczew
ZDR w Piaskach, ul. Lubelska 80, 21-050 Piaski
ZDR w Radzyniu Podlaskim, ul. Rynek 10 a, 21-300 Radzyń Podlaski
ZDR w Rykach, ul. Szkolna 3, 08-500 Ryki
ZDR w Tomaszowie Lubelskim, ul. Żwirki i Wigury 2, 22-600 Tomaszów Lubelski
ZDR w Wisznicach, ul. Wygoda 10, 21-580 Wisznice
ZDR we Włodawie, ul. Piłsudskiego 64, 22-200 Włodawa
ZDR w Zamościu z/s w Sitnie, 22-424 Sitno

Wykaz zbiorów danych osobowych oraz programów służących do ich przetwarzania

L.p.	Zbiór	Program
1.	Kadrowo-płacowy	• Program kadrowo-płacowy KALI • Płatnik • Subiekt • system bankowości elektronicznej VideoTel • MS Office
2.	Szkolenia i doradztwo	• MS Office • arkusz kalkulacyjny o specjalnie przygotowanej formule • PL FADN • Sprawozdawczość pracy doradczej
3.	Działalność wydawnicza	MS Office
4.	Konkursy	MS Office
5.	Klienci	Subiekt
6.	Kontakty służbowe	MS Office

Opis struktury zbiorów danych
wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. **Kadrowo-płacowy**

Zbiór ten obejmuje dane byłych i obecnych pracowników oraz osób świadczących usługi na rzecz administratora danych na innej podstawie niż stosunek pracy - imię i nazwisko osoby, jej adres, numer telefonu, wysokość wynagrodzenia, podstawowe, niezbędne do ustalenia wysokości wynagrodzenia, dane dotyczące stażu pracy, wykształcenia, urlopów i zwolnień, numer dowodu osobistego, numer konta bankowego, numer NIP i PESEL, imiona rodziców, datę i miejsce urodzenia, informacje o odbytych szkoleniach, urlopach, informacje o posiadanych dzieciach, zawartych związkach małżeńskich, a także dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych zwłaszcza w wyniku badań profilaktycznych (wstępnych, okresowych i kontrolnych).

2. **Szkolenia i doradztwo**

Zbiór ten obejmuje następujące dane: nazwisko i imię odbiorcy usługi, adres zamieszkania, numer telefonu, e-mail, numer gospodarstwa, imiona rodziców, PESEL, NIP, NIG, Regon, numer i seria dowodu osobistego, data i miejsce urodzenia, posiadane kwalifikacje, wykształcenie, stan rodziny, stan majątkowy, dane rachunkowe, nr konta.

3. **Działalność wydawnicza**

Zakres danych to: imię i nazwisko, adres, telefon kontaktowy, e-mail

4. **Konkursy**

Zbiór ten zawiera następujące dane: imię, nazwisko, imiona rodziców, data i miejsce urodzenia, adres, PESEL, NIP, zawód, wykształcenie, numer dowodu osobistego, numer telefonu, wiek uczestnika, imię i nazwisko opiekuna prawnego.

5. **Klienci**

Zakres danych ograniczony jest do danych niezbędnych do wystawienia faktury czy rachunku: imię i nazwisko, adres, w przypadku osób prowadzących działalność gospodarczą: nazwa i adres firmy, NIP.

6. **Kontakty służbowe**

Zakres danych obejmuje dane: imię i nazwisko, telefon służbowy, służbowy adres e-mail, miejsce pracy, stanowisko.

Instrukcja ochrony danych osobowych przetwarzanych w systemie informatycznym Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli

1. Podstawa prawna

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z późn. zm.)

2. Przepisy ogólne

1. Instrukcja ochrony danych osobowych przetwarzanych w systemie informatycznym Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli, zwana dalej Instrukcją, opisuje zasady ochrony danych osobowych przetwarzanych w systemie informatycznym oraz postępowanie w przypadku ich naruszenia.
2. Niniejsza instrukcja realizuje Politykę bezpieczeństwa informacji Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli.

3. Definicje

Administrator Danych Osobowych - Dyrektor Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli.

Administrator Systemu Informatycznego - osoba odpowiedzialna za planowanie, konfigurowanie i poprawne funkcjonowanie systemu i sieci teleinformatycznej na terenie Lubelskiego Ośrodka Doradztwa Rolniczego w Końskowoli, zarządzająca również prawami dostępu do sieci poszczególnych jej użytkowników.

Administrator Bezpieczeństwa Informacji - osoba odpowiedzialna za nadzorowanie przestrzegania zasad ochrony danych osobowych ustanowionych zgodnie z Polityką bezpieczeństwa informacji w LODR.

Użytkownik systemu - osoba przetwarzająca merytoryczne dane osobowe w ramach wykonywanych zadań, niezależnie od charakteru zatrudnienia lub wykonywanych prac zleconych.

Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zabieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Osoba uprawniona - pracownik Działu Zastosowań Teleinformatyki.

Naruszenie zabezpieczenia - jakiekolwiek zdarzenie lub działanie, które może stanowić przyczynę utraty zasobów, niezawodności, integralności lub poufności danych.

4. Uprawnienia, podział obowiązków

4.1. Administrator Danych Osobowych odpowiada za:
- bezpieczeństwo systemu informatycznego LODR;
- wyznaczanie zakresu dostępu do zasobów informatycznych dla użytkowników systemu;
- systemy techniczne i sposoby ochrony przed zagrożeniami;
- powoływanie zespołu osób odpowiedzialnych za kontrolowanie przestrzegania zasad bezpieczeństwa informatycznego LODR.

4.2. Administrator Systemu Informatycznego jest odpowiedzialny za:
- konfigurowanie i poprawne funkcjonowanie sieci informatycznej;
- organizację i koordynację działań w zakresie bezpieczeństwa systemów informatycznych;
- kontrolę poszczególnych stanowisk komputerowych;
- zlecanie pracownikom Działu Zastosowań Teleinformatyki wdrażania zadań związanych z przestrzeganiem zasad bezpieczeństwa informatycznego w LODR;
- administrowanie systemami, w których przetwarzane są dane osobowe;
- przyznawanie użytkownikom identyfikatorów i przyznawanie im uprawnień, które wynikają z nadanego upoważnienia do przetwarzania danych osobowych;
- instalowanie, aktualizowanie i konfigurowanie oprogramowania systemowego i aplikacyjnego oraz urządzeń, o ile czynności te nie są wykonywane przez upoważnionych przedstawicieli dostawcy systemu na podstawie zawartej umowy;
- instalowanie i aktualizowanie oprogramowania antywirusowego;
- reagowanie w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych przetwarzanych w systemie;
- tworzenie, rejestrowanie, przechowywanie i archiwizowanie kopii zapasowych baz danych osobowych;
- przygotowywanie urządzeń, dysków i innych elektronicznych nośników informacji, zawierających dane osobowe, do likwidacji, przekazania innemu podmiotowi, konserwacji lub naprawy;
- przekazywania do Administratora Bezpieczeństwa Informacji opisów struktur zbiorów danych, schematów przepływu danych pomiędzy systemami, zawartości poszczególnych pól informacyjnych w aplikacjach oraz wszelkich zmian w tym zakresie;
- zakładanie, modyfikacja lub usuwanie baz danych w systemie oraz realizowanie migracji danych pomiędzy nimi;
- wykonywanie bieżącej konserwacji i przeglądu systemu;
- uaktualnianie kont i uprawnień użytkowników systemu;
- ocenę fachowości i wiarygodności firm informatycznych oraz serwisujących sprzęt.

4.3. Administrator Bezpieczeństwa Informacji odpowiada za:
- nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu zapewnienia bezpieczeństwa danych;
- nadzór nad funkcjonowaniem systemu zabezpieczeń wdrożonych w celu ochrony danych osobowych;
- prowadzenie ewidencji z zakresu ochrony danych osobowych;
- za przegląd i aktualizację dokumentacji przetwarzania danych osobowych;

- nadzór udostępniania danych osobowych odbiorcom danych i innym podmiotom;
- przygotowywanie wniosków zgłoszeń rejestracyjnych i aktualizację zbiorów danych oraz prowadzenie korespondencji z Generalnym Inspektorem Ochrony Danych Osobowych;
- nadzorowanie oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń lub podejrzenia naruszenia;
- przygotowanie materiałów szkoleniowych z zakresu ochrony danych osobowych.

4.4. Kierownik komórki organizacyjnej / Koordynator odpowiada za:
- przestrzeganie bezpieczeństwa systemu informatycznego w podległej komórce organizacyjnej;
- ochronę i zabezpieczenie środków technicznych potrzebnych do przestrzegania bezpieczeństwa systemów informatycznych;
- ochronę sprzętu teleinformatycznego i nadzór na użytkownikami systemu w podległej komórce organizacyjnej.

4.5. Użytkownik systemu jest odpowiedzialny za:
- ochronę i zabezpieczenie powierzonego sprzętu;
- prawidłową eksploatację systemu;
- ochronę sprzętu przed korzystaniem z niego przez osoby niezatrudnione w LODR.

5. Zasady postępowania, opis

5.1. Cele instrukcji

Instrukcja wprowadza zasady postępowania i ochrony w odniesieniu do danych w formie elektronicznej, a w szczególności danych osobowych, które są przetwarzane elektronicznie, jak również sprzętu i oprogramowania tworzącego system informatyczny. Dotyczy to również sieci teleinformatycznej wykorzystywanej do przesyłania i przetwarzania wszelkiego rodzaju danych na potrzeby LODR.

5.2. Zasoby informatyczne LODR podlegające ochronie

Zasoby informatyczne podlegające ochronie:
1. **sprzęt** - komputery, serwery, urządzenia sieciowe, fizyczna sieć komputerowa, połączenia telekomunikacyjne;
2. **oprogramowanie** - programy używane w firmie, systemy operacyjne;
3. **dane** - bazy danych, kopie bezpieczeństwa, logi systemowe oraz wszelkie transmisje tych danych;
4. **pozostałe** - sieć zasilająca, pomieszczenia.

1. **Ochrona sprzętu** będącego zasobem polega na ścisłym przestrzeganiu zasad dotyczących warunków eksploatacji sprzętu, prowadzeniu jego konserwacji zgodnie z przepisami i wymaganiami producenta oraz na ochronie przed kradzieżą, zniszczeniem, uszkodzeniem lub użytkowaniem niezgodnym z przeznaczeniem, a także ochronie przed użytkowaniem przez osoby nieuprawnione.
2. **Ochrona zasobów oprogramowania** polega na przestrzeganiu zasad użytkowania, zabezpieczeniu systemów operacyjnych i programów użytkowych przed nielegalnym kopiowaniem, kradzieżą oraz nieuprawnioną modyfikacją i aktualizacją.
3. **Ochrona danych** (bazy danych, kopie bezpieczeństwa, logi systemowe oraz wszelkie transmisje tych danych) polega na zabezpieczeniu informacji wprowadzonej,

modyfikowanej, przetwarzanej i przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą, niewłaściwym wykonywaniem kopii bezpieczeństwa, nieuprawnioną modyfikacją lub nieautoryzowanym usunięciem.

4. **Ochrona pozostałych zasobów** (sieć zasilająca, pomieszczenia) polega na zapewnieniu ciągłości zasilania oraz odpowiednich pomieszczeń z zabezpieczeniami dla zasobów sprzętowych, oprogramowania i danych.

Zasady nadzoru nad sprzętem informatycznym, których przestrzeganie zapewnia:

- prawidłowy proces przygotowania sprzętu informatycznego oraz jego wymiany,
- prawidłową obsługę awarii sprzętu informatycznego,
- zasady okresowego przeglądu sprzętu informatycznego,
- nadzór nad legalnością używanego w LODR oprogramowania i systemów operacyjnych;

zostały określone w procedurze systemu zarządzania jakością P-SZJ/005 Nadzór nad sprzętem informatycznym i odnoszą się w szczególności do:

- zarządzania sprzętem informatycznym,
- instalowania nowego sprzętu informatycznego,
- zmiany w konfiguracji istniejącego sprzętu informatycznego,
- zwrotu sprzętu informatycznego,
- okresowej kontroli stanu technicznego sprzętu informatycznego,
- likwidacji sprzętu informatycznego i oprogramowania,
- postępowania w przypadku awarii sprzętu informatycznego.

5.3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania ich w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora osoby i właściwego hasła.
2. Administrator Systemu Informatycznego jest odpowiedzialny za nadawanie uprawnień do przetwarzania danych i rejestrowanie ich w systemie informatycznym.
3. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.
4. Identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może zostać przydzielony innej osobie.
5. Pracownicy są odpowiedzialni za zachowanie poufności swoich identyfikatorów i haseł.
6. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Administratora Bezpieczeństwa Informacji.
8. Przy wyborze hasła obowiązują następujące zasady:
   - minimalna długość hasła - 8 znaków;
   - zakazuje się stosować: haseł, które użytkownik stosował uprzednio, swojego identyfikatora w jakiejkolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku (numer telefonu, numer rejestracyjny samochodu, numeru PESEL, itp.);

- tworzone hasło nie może być sekwencją kolejnych liter klawiatury (np. „1234567890", „ASDFGHJK"„asdfghjk", „QWERTYUIOP", „qwertyui", „zxcvbnm,");
- należy stosować: hasła zwierające kombinacje liter i cyfr, hasła zawierające znaki specjalne: (.,();'@, #, & itp.), o ile system informatyczny i oprogramowanie na to pozwala.

9. Zmiany hasła nie wolno zlecać innym osobom.
10. W razie zapomnienia hasła należy ten fakt zgłosić do Administratora Systemu Informatycznego.

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

1. Rozpoczęcie pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu.
2. Przed opuszczeniu stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i systemu operacyjnego.
3. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wylogować się z systemu operacyjnego i zamknąć system.
4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania i systemu operacyjnego.

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

1. Administrator Systemu Informatycznego lub wyznaczeni przez niego pracownicy LODR zobowiązani są do tworzenia kopii zapasowych zbiorów danych na nośnikach informacji (backup) według zasad określonych w instrukcji użytkowania systemu/aplikacji. Jeżeli instrukcja użytkowania systemu/aplikacji nie określa zasad tworzenia kopii zapasowych, to zasady te określa w formie wytycznych Administrator Systemu Informatycznego.
2. Zasady, o których mowa powyżej powinny zawierać postanowienia dotyczące:
   a) częstotliwości tworzenia kopii zapasowych dla poszczególnych rodzajów zbiorów danych i programów;
   b) metod tworzenia kopii zapasowych: typ nośników, narzędzia programowe i urządzenia do ich tworzenia;
   c) miejsca przechowywania i dostępu do kopii bezpieczeństwa;
   d) okresów rotacji kopii bezpieczeństwa oraz całkowitego czasu użytkowania poszczególnych rodzajów nośników;
   e) procedury kasowania i likwidacji nośników zawierających dane osobowe;
   f) osób odpowiedzialnych za poszczególne fazy tworzenia i przechowywania kopii roboczych oraz realizujące poszczególne czynności w tym zakresie.

5.6. Sposób przechowywania kopii zapasowych

Nośniki informacji, na których składowane są kopie zapasowe powinny być przechowywane w innych pomieszczeniach, niż te, w których odbywa się przetwarzanie informacji. Pomieszczenia te powinny spełniać odpowiednie warunki oraz posiadać zabezpieczenia chroniące przed zniszczeniem (pożar, zalanie wodą, kradzieżą) i nieuprawnionym dostępem. Ponadto powinny być one zlokalizowane poza zasięgiem silnych pól elektromagnetycznych.

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

1. Zgodnie z procedurą P-SZJ/005 Nadzór nad sprzętem informatycznym, okresowe kontrole stanu technicznego sprzętu informatycznego i legalności oprogramowania przeprowadzane są przez osoby uprawnione. Kontrola polega na porównaniu zgodności zawartości wszystkich stacji roboczych z prowadzoną ewidencją sprzętu informatycznego oraz weryfikacji obecności i ocenie stanu technicznego całego sprzętu informatycznego LODR.
2. W przypadku konieczności przeprowadzenia okresowych przeglądów stanu technicznego przez firmy zewnętrzne, osoba uprawniona zobowiązana jest do nadzorowania terminu rozpoczęcia tych prac, ich przebiegu oraz zakończenia i przechowywania protokołów potwierdzających wykonanie takich przeglądów.
3. W przypadku stwierdzenia, że dany sprzęt jest wadliwy należy dokonać jego naprawy lub wymiany. Za nadzór nad naprawą gwarancyjną i pogwarancyjną sprzętu odpowiedzialne są osoby uprawnione.
4. Okresowa kontrola stanu technicznego oprogramowania prowadzona jest raz do roku. Dowodem przeprowadzenia kontroli jest zapis w Karcie informacyjnej zestawu komputerowego.
5. Za nadzór nad terminową realizacją przeglądu odpowiada osoba uprawniona.

5.8. Sposób zabezpieczenia systemu informatycznego przed wrogim oprogramowaniem

Bieżące i bezpośrednie sprawdzanie obecności wirusów komputerowych, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego i kradnącego hasła, niszczącego dane i strukturę systemu odbywa się przy zastosowaniu zainstalowanego na każdej stacji roboczej, aktualizowanego na bieżąco, programu antywirusowego automatycznie monitorującego występowanie wirusów, koni trojańskich, robaków komputerowych, oprogramowania szpiegującego, oprogramowania kradnącego hasła podczas operacji na plikach.

5.8.1. Czynności

1. Instalowanie oprogramowania antywirusowego oraz jego bieżącą aktualizację wykonuje Administrator Systemu Informatycznego lub inne osoby uprawnione.
2. O każdorazowym wykryciu wirusa lub konia trojańskiego przez oprogramowanie monitorujące użytkownik jest zobowiązany niezwłocznie powiadomić Administratora Systemu Informatycznego lub osobę uprawnioną. Po usunięciu wirusa lub innego niebezpiecznego oprogramowania, Administrator Systemu Informatycznego lub osoba uprawniona sprawdza system oraz przywraca go do pełnej funkcjonalności i sprawności.
3. W ramach ochrony przed wrogim oprogramowaniem Administrator Systemu Informatycznego lub osoba uprawniona stosuje logiczne lub fizyczne urządzenia firewall.
4. Dyski lub inne informatyczne nośniki zawierające dane osobowe przetwarzane w LODR są przechowywane w sposób uniemożliwiający dostęp do nich osobom innym niż użytkownicy.
5. Żadne nośniki informacji zawierające dane osobowe nie są udostępniane poza obszar, w którym są przetwarzane dane osobowe.
6. Zapis nie dotyczy sytuacji, o której mowa w § 29 pkt 1 ustawy o ochronie danych osobowych, tzn. udostępniania posiadanych w zbiorze danych osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

5.8.2. Wymagania sprzętowo-organizacyjne

1. Użytkownicy systemu są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitora.
2. Komputery powinny zostać ustawione w taki sposób, aby osoby postronne miały utrudniony dostęp do portów zewnętrznych lub przynajmniej dostęp do portów zewnętrznych był pod kontrolą wizualną użytkowników systemu.
3. Osoby nieuprawnione do dostępu do danych osobowych w LODR mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe w LODR wyłącznie w obecności użytkownika systemu.
4. Decyzję o instalacji na stacji roboczej obsługującej przetwarzanie danych osobowych w LODR jakiegokolwiek oprogramowania systemowego lub użytkowego podejmuje Administrator Systemu Informatycznego.

6. Postępowanie w przypadku naruszenia ochrony danych osobowych przetwarzanych w systemie informatycznym

1. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:
   a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Pracownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym LODR zobowiązany jest, do niezwłocznego poinformowania o tym Administratora Systemu Informatycznego, Administratora Danych Osobowych, a w przypadku jego nieobecności Administratora Bezpieczeństwa Informacji.
3. Administrator, który stwierdził lub uzyskał informację wskazującą na naruszenie zasad ochrony tych danych zobowiązany jest do niezwłocznego:
   1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu zasad ochrony danych osobowych lub czasu samodzielnego wykrycia tego faktu,
   2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
   3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych,
   4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:
      a) fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej,
      b) wylogowania użytkownika podejrzanego o naruszenie zasad ochrony danych,
      c) zmianę hasła użytkownika, poprzez którego uzyskano nielegalny dostęp, w celu uniknięcia ponownej próby uzyskania takiego dostępu;
   5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia zasad ochrony danych osobowych,
   6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

4. Po przywróceniu normalnego stanu systemu informatycznego należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
   a) Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
   b) Jeżeli przyczyną zdarzenia była infekcja wirusem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
   c) Jeżeli przyczyną zdarzenia okazało się zaniedbanie ze strony użytkownika systemu, należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy.
5. Administrator Systemu Informatycznego zobowiązany jest do przygotowania szczegółowego raportu o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia, przekazania go Administratora Bezpieczeństwa Informacji.
6. Administrator Bezpieczeństwa Informacji zobowiązany jest do przeprowadzania analiz raportów pochodzących od Administratora Systemu Informatycznego.

7. Postanowienia końcowe

1. Do spraw nieuregulowanych w Instrukcji stosuje się przepisy o ochronie danych osobowych.
2. Instrukcja nie wyłącza stosowania innych przepisów dotyczących zabezpieczenia w LODR.