ZARZĄDZENIE Nr 17.2018

NADLEŚNICZEGO NADLEŚNICTWA CIECHANÓW
z dnia 28.11.2018r.

w sprawie wprowadzenia do stosowania „Polityki ochrony danych osobowych"
w Nadleśnictwie Ciechanów

ZNAK SPRAWY: N. 0210.20.2018

Na podstawie § 22 pkt 3 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe, stanowiącego załącznik do Zarządzenia Nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. w sprawie nadania Statutu Państwowemu Gospodarstwu Leśnemu Lasy Państwowe, Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), oraz ustawy z dnia 10 maja 2018r o ochronie danych osobowych (Dz. U. 2018 poz. 1000)

§ 1.

Wprowadzam do stosowania „Politykę Ochrony Danych Osobowych" w Nadleśnictwie Ciechanów – stanowiącą załącznik nr 1. Do niniejszego Zarządzenia.

§ 2.

Zobowiązuje wszystkich pracowników, którzy w ramach swoich obowiązków przetwarzają dane osobowe do wnikliwego zapoznania się z zapisami „Polityki ochrony danych osobowych" i potwierdzenia tego faktu przez złożenie stosownego oświadczenia wg wzoru stanowiącego załącznik nr 2 niniejszego Zarządzenia. Oświadczenia należy przekazać do stanowiska NP.

§ 3.

Traci moc Zarządzenie nr 9/2012 z dnia 29.05.2012r w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji w Nadleśnictwie Ciechanów.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

NADLEŚNICZY
Nadleśnictwa Ciechanów
Wojciech Kamiński

Otrzymują (drogą elektroniczną):

- Pracownicy Nadleśnictwa Ciechanów
- Administrator SILP (do umieszczenia na serwerze wymiany danych)
- Inspektor Ochrony Danych

Załącznik nr 1.

do Zarządzenia nr 17.2018 z dnia

28.11.2018r. znak spr. N.0210.20.2018

Polityka ochrony danych osobowych

w NADLEŚNICTWIE CIECHANÓW

Metryka dokumentu

Metryka dokumentu		
Tytuł		Polityka Ochrony Danych w Nadleśnictwie Ciechanów
Wersja bieżąca		1.0
Data ostatniej modyfikacji		2018.11.28 (data wprowadzenia)
Opracował		Rafał Nalewajko, Piotr Sarnowski
Ostatni modyfikował		
Zaakceptował		Wojciech Kamiński
Historia zmian dokumentu		
Wersja	Data wersji	Uwagi
1.0	2018.11.28	

Spis treści

Cel Polityki

Polityka ochrony danych osobowych, zwana dalej Polityką, określa zasady przetwarzania danych osobowych, których administratorem jest Nadleśnictwo Ciechanów, w celu ich zabezpieczenia adekwatnie do ryzyka i zidentyfikowanych zagrożeń oraz uzyskania zgodności z wymaganiami przepisów prawa w obszarze ochrony danych osobowych.

1. Podstawa prawna

Zasady przedstawione w Polityce zostały oparte na wymaganiach Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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).

Powołuje się Zarządzeniem Nadleśniczego osobę do pełnienia funkcji Inspektora Ochrony Danych. Zakres odpowiedzialności Inspektora Ochrony Danych został określony w pkt. 5 niniejszej Polityki.

Wybrane akty prawne normujące działanie Nadleśnictwa:

1. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 (Dz. U. 2018 poz. 1000)
2. Rozporządzenie Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 1 lipca 2014 r. w sprawie szczegółowych zasad współdziałania Lasów Państwowych z Policją (Dz.U. 2014, poz.910).
3. Ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (Dz.U. 2015, poz. 1930z późń. zm.).
4. Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2013 r. poz. 628, z późń. zm.).

2. Wdrożenie Polityki

1) Polityka określa podstawowy standard bezpieczeństwa danych osobowych oparty na przepisach RODO.
2) Wszystkie pracownicy są zobowiązani do stosowania reguł zawartych w niniejszej Polityce w odniesieniu do przetwarzanych danych osobowych.
3) Zasady określone w niniejszej Polityce są obligatoryjnym obszarem wiedzy, z którym powinni być zapoznawani wszyscy pracownicy i współpracownicy Nadleśnictwa.

3. Definicje i skróty

Termin	Znaczenie
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnie rozporządzenie o ochronie danych)
Klauzula zgoda podmiotu danych	Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

Termin	Znaczenie
Klauzula informacyjna	Informowanie osób, których dane dotyczą, o wykorzystywaniu ich danych osobowych (prowadzeniu operacji przetwarzania) i celach, dla których jest ono prowadzone oraz jest niezbędne dla zapewnienia rzetelności i przejrzystości przetwarzania danych osobowych.
Administrator danych	Nadleśnictwo Ciechanów, która ustala cele i sposoby przetwarzania danych osobowych.
Podmiot przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych.
Inspektor Ochrony Danych (IOD)	Osoba fizyczna powołana zarządzeniem Nadleśniczego do wspierania Administratora Danych w przestrzeganiu postanowień RODO.
Kierownik Projektu	Osoba odpowiedzialna za planowanie, realizację i zamykanie projektu. Podstawowym zadaniem kierownika projektu jest zapewnienie osiągnięcia założonych celów projektu.
Kierownik jednostki/ komórki organizacyjnej	Kierownika lub samodzielne stanowisko bezpośrednio podległe pod Nadleśniczego.
Dane osobowe	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, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
Zbiór danych osobowych	Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
Przetwarzanie danych osobowych	Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
Naruszenie ochrony danych osobowych	Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Termin	Znaczenie
Profilowanie	Dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było 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,
Ograniczenie przetwarzania danych osobowych	Oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
Specjalne kategorie danych	Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
Pracownik	Osoba fizyczna zatrudniona w Nadleśnictwie na podstawie umowy o pracę lub powołania.
Współpracownik	Osoba fizyczna współpracująca ze Nadleśnictwem w oparciu o umowę zlecenia, o dzieło i inne umowy o charakterze cywilnoprawnym, jak też praktykant, stażysta, wolontariusz, pracownik tymczasowy - wykonujący pracę lub realizujący czynności zlecone na rzecz Nadleśnictwa.
System teleinformatyczny	Wydzielony zespół współpracujących ze sobą urządzeń oraz oprogramowania, przetwarzający dane osobowe w postaci elektronicznej.

4. Status Inspektora Ochrony Danych (IOD)

1) Inspektor Ochrony Danych podlega bezpośrednio Nadleśniczemu.
2) IOD jest właściwie i niezwłocznie włączany przez Administratora Danych we wszystkie kwestie związane z przetwarzaniem danych poprzez:
   a) informowanie o wszystkich sprawach związanych z przetwarzaniem danych osobowych odpowiednio wcześniej, umożliwiając zajęcie stanowiska;
   b) uwzględnianie stanowiska przy wszystkich przedsięwzięciach związanych z przetwarzaniem danych osobowych;

c) uczestnictwo przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych; konsultacje w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi .

3) Administrator Danych w celu prawidłowego wykonywania zadań przez IOD zapewnia:
   a) wsparcie ze strony Administratora Danych;
   b) niezbędne wsparcie osobowe, finansowe, techniczne, infrastrukturalne;
   c) dostęp do wszystkich jednostek/komórek organizacyjnych (np. kadr, IT, ochrony etc.), celem stworzenia przepływu informacji między tymi jednostkami/komórkami organizacyjnymi a IOD;
   d) kontakt z osobami fizycznymi, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących;
   e) środki finansowe na pogłębianie wiedzy z zakresu ochrony danych osobowych poprzez udział w szkoleniach, warsztatach, forach poświęconych ochronie danych etc..
4) IOD w ramach wypełniania zadań nie otrzymuje instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte. IOD nie może zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych.
5) Inspektor Ochrony Danych nie jest odwoływany, ani karany przez Administratora Danych za wypełnianie swoich zadań. IOD może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków IOD (np. kradzież, nękanie fizyczne i psychiczne, molestowanie seksualne, ciężkie naruszenie obowiązków).
6) Inspektor Ochrony Danych może wykonywać inne zadania, obowiązki powierzone przez Administrator Danych, jeśli one nie wpływają negatywnie na wykonywanie przez niego obowiązków IDO oraz nie powodują konfliktu interesów.
7) IOD jest zobowiązany do zachowania tajemnicy co do wykonywania swoich zadań zgodnie z prawem Unii Europejskiej i prawem krajowym.

5. Odpowiedzialność

1) Odpowiedzialność **Administrator danych -** jest odpowiedzialny za wdrożenie skutecznych środków technicznych i organizacyjnych uwzględniających charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Administrator danych zobowiązany jest wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z przepisami prawa.
2) **Inspektor Ochrony Danych (IOD)** – osoba powołana zarządzeniem Nadleśniczego, realizująca następujące zadania:
   a) informowanie Administratora danych, podmiotu przetwarzającego oraz pracowników i współpracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich z mocy rozporządzenia RODO oraz innych przepisów Unii Europejskiej i przepisów krajowych o ochronie danych i doradzenia im w tej sprawie;
   b) monitorowanie przestrzegania postanowień RODO, innych przepisów Unii Europejskiej i przepisów krajowych o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego, w dziedzinie ochrony danych osobowych, w tym podział obowiązków,

działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do skutków dla ochrony danych (PIA) oraz monitorowanie jej wykonania zgodnie z art. 35 RODO (ocena skutków dla ochrony danych);
d) współpraca z organem nadzorczym ochrony danych osobowych;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenia konsultacji we wszystkich innych sprawach;
f) wypełnia zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;
g) prowadzi, z upoważnienia Administratora danych, rejestr czynności przetwarzania danych osobowych.

3) **Administrator Systemu Informatycznego (ASI)**– osoba odpowiedzialna za administrowanie Systemem teleinformatycznym, zgodnie z wytycznymi kierunkowymi określanymi przez Dysponenta Systemu teleinformatycznego. Administratora Systemu wyznacza Kierownik jednostki IT. Administrator jest odpowiedzialny w szczególności za:
   a) wdrożenie adekwatnych zabezpieczeń organizacyjnych i technicznych w nadzorowanym Systemie teleinformatycznym przetwarzającym dane osobowe;
   b) bieżącą administrację Systemem teleinformatycznym służącym do przetwarzania danych osobowych, w tym realizację czynności związanych z jego prawidłowym funkcjonowaniem/utrzymaniem;
   c) zgodność funkcjonowania Systemu teleinformatycznego z przepisami prawa w zakresie ochrony danych osobowych;
   d) zgłaszanie niezwłocznie IOD każdego wykrytego przypadku naruszenia bezpieczeństwa danych osobowych oraz uczestniczy w wyjaśnianiu naruszenia, w tym ustaleniu przyczyn i ewentualnych skutków;
   e) zgłaszanie IOD wszelkich zmian w Systemie teleinformatycznym wynikających z procesów zarządzania zmianą mających bezpośredni bądź pośredni wpływ na procesy przetwarzania danych osobowych w systemie.

4) **Kierownik jednostki/organizacyjnej komórki organizacyjnej** – jest odpowiedzialny za wdrażanie odpowiednich zabezpieczeń organizacyjnych, fizycznych, osobowych i technicznych w nadzorowanej jednostce organizacyjnej /komórce organizacyjnej, a także za prawidłowy przebieg procesów związanych z przetwarzaniem danych osobowych w obszarze swojej jednostki/komórki. W ramach powyższego działania odpowiada za:
   a) raportowanie Inspektorowi Ochrony Danych wszelkich zmian w procesach przetwarzających dane osobowe (takich jak zakres danych, cel przetwarzania, odbiorcy danych);
   b) uwzględnienia ochrony danych osobowych w fazie projektowania nowych rozwiązań lub wprowadzania znaczących modyfikacji w już istniejących poprzez przeprowadzenie obowiązkowej konsultacji z IOD;

c) konsultowanie treści zgód i obowiązków informacyjnych przed rozpoczęciem pozyskiwania lub modyfikacji zakresu pozyskiwania danych osobowych;
d) dopełnienie obowiązku konsultacji/zaopiniowania umowy powierzenia przez IOD;
e) dopełnienie obowiązku przeprowadzenia analizy czy podmiot, któremu powierzone maja zostać dane osobowe zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane osobowe dotyczą;
f) niezwłocznego zgłaszania naruszeń ochrony danych osobowych;
g) udzielanie IOD wyjaśnień w sprawach dotyczących przetwarzania danych osobowych, w tym naruszeń bezpieczeństwa danych osobowych w podległej jednostce.

5) **Pracownicy i współpracownicy** – są zobowiązani do przestrzegania zasad niniejszej Polityki oraz procedur ochrony danych, a także do niezwłocznego zgłaszania zauważonych naruszeń ochrony danych osobowych.

6. Zasady ochrony danych osobowych

1) Nadleśnictwo zobowiązane jest do ochrony przetwarzanych danych osobowych oraz realizacji praw osób, których dane są przetwarzane.
2) Dane osobowe przetwarzane muszą być:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
   c) adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne dla realizacji celów, dla których są przetwarzane;
   d) prawidłowe i w razie potrzeby uaktualniane;
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą;
   f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych,
   g) w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

7. Przesłanki przetwarzania danych osobowych

1) W Nadleśnictwie dane osobowe mogą być przetwarzane tylko gdy:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych
   b) w jednym lub większej liczbie określonych celów;

c) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
d) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
e) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
f) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
g) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (np. prowadzenie marketingu bezpośredniego własnych produktów i usług), z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2) Przetwarzanie specjalnych kategorii danych jest zabronione, chyba że występują przesłanki, o których mowa w RODO (art. 9).

8. Prawa osoby, której dane osobowe są przetwarzane.

1) Procedurę realizacji praw osób, których dotyczą dane osobowe określa *Załącznik nr 5* do niniejszej Polityki
2) Każda osoba, której dane osobowe są przetwarzane ma:

a) **Prawo dostępu do danych** osobowych - osoba, której dane osobowe dotyczą ma prawo do uzyskania następujących informacji o:
   a) celach przetwarzania;
   b) kategoriach przetwarzanych danych osobowych;
   c) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;
   e) prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   f) prawie wniesienia skargi do organu nadzorczego;
   g) źródle danych, jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą;
   h) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Dodatkowo, osoba, której dane dotyczą może żądać kopii danych osobowych przetwarzanych przez Nadleśnictwo.

b) **Prawo do sprostowania danych** osobowych – Osoba, której dane osobowe dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych;

c) **Prawo do usunięcia danych osobowych („prawo do bycia zapomnianym")** – Osoba, której dane osobowe dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator 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;
   d) dane osobowe były przetwarzane niezgodnie z prawem;
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie polskim;
   f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

d) **Prawo do ograniczenia przetwarzania** – Osoba, której dane osobowe dotyczą, ma prawo żądania ograniczenia przetwarzania w następujących przypadkach:
   a) osoba, której dane osobowe dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane osobowe dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane osobowe dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   d) osoba, której dane osobowe dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

e) **Prawo do przenoszenia danych osobowych** – Osoba, której dane osobowe dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:
   a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz
   b) przetwarzanie odbywa się w sposób zautomatyzowany.

f) **Prawo do sprzeciwu** - Osoba, której dane osobowe dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, w tym profilowania. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych

prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

9. Obowiązki Nadleśnictwa.

1) Nadleśnictwo dopełnia obowiązku informacyjnego **podczas** zbierania danych. Treść klauzuli informacyjnej konsultuje się z IOD przed rozpoczęciem przetwarzania danych. Przy zmianie celu i zakresu przetwarzania danych wymagana jest ponowna konsultacja z IOD. W przypadku pozyskania danych z innych źródeł niż od osoby, informacje zawarte w klauzuli informacyjnej muszą zostać przekazane tej osobie przy pierwszej komunikacji, nie później jednak niż w ciągu miesiąca od pozyskania tych danych.
2) Sposób pozyskiwania, gromadzenia i archiwizacji **zgód na przetwarzanie danych osobowych** oraz sposób zarządzania tymi zgodami, uwzględniający różne cele przetwarzania oraz prawo do odwołania zgody. Należy uwzględnić, że odwołanie zgody powinno być równie łatwe jak jej wyrażenie. Procedurę określa Załącznik 4 do niniejszej Polityki.
3) Administrator danych lub Podmiot Przetwarzający zobowiązany jest do **uwzględnienia ochrony danych osobowych w fazie projektowania** nowych rozwiązań lub wprowadzania znaczących modyfikacji w już istniejących. Administrator danych lub Podmiot Przetwarzający wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.
4) Administrator Danych upoważnienia do przetwarzania danych osobowych pracowników i współpracowników. Upoważnienie (Załącznik 6 do niniejszej Polityki) przed dopuszczeniem pracownika lub współpracownika do przetwarzania danych osobowych, Rejestr upoważnień (Załącznik 7 do niniejszej Polityki prowadzi IOD.
5) Nadleśnictwo uwzględniania tematykę ochrony danych osobowych oraz zasady wynikających z niniejszej Polityki w realizowanych programach szkoleniowych np. e-learning, szkolenia stanowiskowe, newsletter z najważniejszymi wydarzeniami w zakresie ochrony danych osobowych.
6) Każdy nowy Pracownik i Współpracownik powinien zostać przeszkolony z zasad ochrony danych osobowych w Nadleśnictwie.
7) Pracownik i Współpracownik nie może zostać dopuszczony do przetwarzania danych osobowych przed odbyciem szkolenia.
8) Bezpośredni przełożony Pracownika lub Współpracownika odpowiada za zapewnienie powyższego szkolenia dla nadzorowanych osób.

9) Osoba upoważniona do przetwarzania danych osobowych, zobowiązana jest odbyć szkolenie przypominające nie rzadziej niż raz na dwa lata z zasad dotyczących ochrony danych osobowych, przeprowadzone przez IOD w Nadleśnictwie,
10) Oświadczenia o zachowaniu w poufności załącza się wraz z upoważnieniem do akt osobowych Pracownika lub do dokumentacji stanowiącej podstawę nawiązania współpracy w przypadku Współpracownika (Załącznik nr 6 do niniejszej Polityki)
11) W celu ewidencjonowania procesów przetwarzających danych osobowe administrator danych prowadzi w postaci elektronicznej rejestr czynności przetwarzania – administratora danych (Załącznik 2 do niniejszej Polityki) i na żądanie udostępnia go organowi nadzorczemu.
12) Kierownicy jednostek/komórek organizacyjnych są odpowiedzialni za aktualizację informacji wymaganych w rejestrze czynności przetwarzania w zakresie działania danej jednostki/komórki organizacyjnej.
13) W celu ewidencjonowania czynności przetwarzania, które zostały powierzone Nadleśnictwo. IOD prowadzi w postaci elektronicznej rejestr kategorii czynności (Załącznik 3 do niniejszej Polityki).

10. Ocena skutków dla ochrony danych osobowych - Privacy Impact Assessment (PIA)

1) Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, IOD przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (PIA). Uznaje się, że ryzyko naruszenia praw i wolności osób fizycznych może być duże w szczególności w przypadku spełnienia 2 spośród poniższych kryteriów:
   a) Ewaluacja lub ocena, w tym profilowanie i przewidywanie, szczególnie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą".
   b) Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne lub podobne istotne skutki.
   c) Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania i kontroli osób, których dane dotyczą.
   d) W ramach procesu przetwarzane są szczególne kategorie danych lub dane dotyczące wyroków skazujących i naruszeń prawa.
   e) Dane przetwarzane są na dużą skalę.
   f) Dokonano porównania lub połączenia zestawów danych: na przykład pochodzących z dwóch lub większej liczby operacji przetwarzania prowadzonych w różnych celach i/lub przez różnych administratorów danych,
   g) Dane dotyczące osób wymagających szczególnej opieki, np. pracownicy, dzieci, osób chorych psychicznie, osób ubiegających się o azyl lub osób starszych, pacjentów, lub w każdym przypadku, gdy można ustalić brak równowagi w relacji między pozycją osoby, której dane dotyczą, a administratora.

h) Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych.
i) Transgraniczne przekazywanie danych poza Unię Europejską.
j) Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy.

2) Ocena PIA zawiera co najmniej:
   a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Nadleśnictwo;
   b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, oraz
   d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
3) Żaden projekt, w ramach którego będą realizowane operacje przetwarzania danych osobowych nie może zostać uruchomiony przez Nadleśnictwo bez określenia wymagań bezpieczeństwa w stosunku do przedmiotowych danych, w szczególności w ramach przeprowadzenia oceny PIA, o ile ocena PIA jest wymagana na podstawie ust.10.1 niniejszej Polityki.
4) Nadleśnictwo informuje IOD o celu i zakresie danych, które będą przetwarzane w ramach planowanego projektu i umożliwia mu ustosunkowanie się do ich adekwatności.
5) IOD przygotowuje plan działania, którego celem jest wdrożenie mechanizmów zapewniających bezpieczeństwo danych osobowych w projekcie.
6) Przetwarzania danych osobowych w projekcie może się rozpocząć dopiero po implementacji określonych w planie działania środków bezpieczeństwa.
7) W każdym innym przypadku, gdy poza trybem projektowym wprowadzane są nowe mechanizmy przetwarzania danych osobowych lub w istotny sposób modyfikowane obowiązujące mechanizmy, osoba odpowiedzialna za te działania jest zobowiązana do skonsultowania tej operacji z IOD.

11. Ochrona danych osobowych w umowach i projektach

1) Żaden projekt, w ramach którego będą realizowane operacje przetwarzania danych osobowych nie może zostać uruchomiony bez określenia wymagań bezpieczeństwa w stosunku do przedmiotowych danych osobowych, w szczególności w ramach przeprowadzenia oceny PIA, o ile ocena PIA jest wymagana na podstawie ust. 10.1 niniejszej Polityki.
2) Przed nawiązaniem współpracy z Podmiotem przetwarzającym jednostka/komórka merytoryczna jest zobowiązana przeanalizować czy zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane osobowe dotyczą. W tym celu należy przeprowadzić analizę, w wyniku której Nadleśnictwo przedstawia potencjalnemu

podmiotowi Przetwarzającemu wymagania w zakresie bezpieczeństwa danych osobowych. W tym:

-wskazuje oczekiwane mechanizmy organizacyjne i techniczne zabezpieczające dane osobowe

- wskazuje warunki udzielenia szczegółowej lub ogólnej zgody w zakresie korzystania z usług innego Pomiotu Przetwarzającego (podwykonawstwo);

-wskazuje czy potencjalny Podmiot przetwarzający powinien wykazać się posiadaniem certyfikatu na zgodność z RODO, ISO 27001 lub analogicznym certyfikatem bezpieczeństwa informacji.

3) Zakres wymagań bezpieczeństwa danych osobowych w zakresie środków technicznych i organizacyjnych dla Wykonawcy, jednostka merytoryczna zobowiązana jest uzgodnić z IOD.
4) W przypadku, gdy analiza, o której mowa w ust. 12.2 wykaże spełnianie wymagań, o których mowa w ust. 12.2. przez przyszły Podmiot Przetwarzający przekazane informacje uzupełnia się w Umowie powierzenia danych osobowych
   a) Wzór zapisów Umowy powierzenia stanowi Załącznik nr 1 do niniejszej Polityki. Możliwe jest odstąpienie od stosowanego wzoru, pod warunkiem, że całość uregulowanych w nim zagadnień zostanie w umowie ujęta.
   b) Każda umowa powierzenia musi zostać zaopiniowana przez IOD. Za dopełnienie obowiązku zaopiniowania umowy z IOD odpowiedzialny jest kierownik jednostki/komórki organizacyjnej odpowiedzialnej za realizację umowy.
5) Wszystkie umowy, w ramach których będzie miało miejsce powierzenie przetwarzania danych osobowych lub ich udostępnienie powinny być zgodne z RODO.

12. Transfer danych osobowych do państwa trzeciego

1) **Przebieg procesu:**
   a) Co do zasady transfer danych osobowych do państwa trzeciego jest zabroniony.
   b) Zgodę na transfer danych wyraża zawsze IOD.
   c) W przypadku transferu danych osobowych poza Europejski Obszar Gospodarczy, Nadleśnictwo weryfikuję czy strona otrzymująca dane spełnia wymagania RODO i prawa kraju, w którym znajduje się administrator danych.

13. Naruszenia ochrony danych osobowych

1) Każdy pracownik, współpracownik, który poweźmie wiadomość o naruszeniu zasad bezpieczeństwa osobowego, bądź posiada informację (domniema o naruszeniu systemu przez różne nietypowe symptomy) mogącą mieć wpływ na bezpieczeństwo ochrony danych osobowych jest zobowiązany ten fakt niezwłocznie zgłosić do IOD oraz bezpośredniego przełożonego.
2) Administrator SILP informacje o naruszeniu przesyła do IOD.
3) Zgłoszenie do IOD odbywa drogą e-mailową i telefoniczną. W siedzibie Nadleśnictwa w miejscach do tego wyznaczonych umieszcza się dane kontaktowe do IOD . Adres emaliowy IOD to

   ciechanow@iod.expert

4) Osoba zgłaszająca naruszenie do momentu podjęcia czynności IOD lub osoby upoważnionej przez Administratora Danych ma obowiązek:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia (o ile istnieje taka możliwość), a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców naruszenia;
   b) rozważyć wstrzymanie bieżącej pracy w celu zabezpieczenia miejsca zdarzenia;
   c) zaniechać (jeśli to jest możliwe) dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia;
   d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu;
   e) zastosować się do innych instrukcji, regulaminów, polityk, procedur, jeśli odnoszą się one do zaistniałego przypadku;
   f) udokumentować wstępnie zaistniałe naruszenie;
5) IOD podejmuje czynności niezbędne do wyjaśnienia naruszenia bezpieczeństwa danych osobowych w szczególności;
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości działania Nadleśnictwa i bezpieczeństwo danych osobowych.
   b) wyjaśnia czy incydent był spowodowany (czynnikami zewnętrznymi lub wewnętrznymi; czynnikiem ludzkim; działaniami celowymi; działaniami niezamierzonymi):
      a) niewłaściwym działaniem lub użyciem systemów informatycznych;
      b) błędami wynikającymi z niekompletnych lub niewłaściwych danych biznesowych;
      c) naruszeniem poufności i integralności danych osobowych;
6) IOD ma prawo i obowiązek żądać składania na piśmie wyjaśnień z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym incydencie bezpieczeństwa danych.
7) Wszystkie działania wyjaśniające dotyczące incydentów naruszenia bezpieczeństwa danych osobowych, które mogą spowodować straty biznesowe, wizerunkowe, prowadzi się na kopiach materiału dowodowego.
8) Po wyczerpaniu niezbędnych środków doraźnych IOD zasięga niezbędnych opinii i uruchamia przedsięwzięcia postępowania naprawczego mi przedstawia informacje oraz informuje Administratora Danych.
9) W przypadku naruszenia danych osobowych, Administrator Danych w porozumieniu z IOD, bez zbędnej zwłoki (w miarę możliwości, nie później niż w 72 godziny po stwierdzeniu naruszenia – zgłasza je Organowi Nadzorczemu) – chyba że naruszenie jest mało prawdopodobne, by skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
10) Zgłoszone naruszenia ochrony danych są rejestrowane w Rejestrze naruszeń – zgodnie z załącznikiem nr 8.

14. Udostępnianie danych osobowych

1) Dane osobowe mogą zostać udostępnione jedynie w przypadku gdy jest ku temu podstawa prawna lub za zgodą podmiotu danych.
2) W przypadku wątpliwości co do podstaw udostępnienia lub zakresu udostępnianych danych,
3) IOD prowadzi rejestr odbiorców, którym udostępniono dane osobowe.
4) Każdorazowo należy zapewnić bezpieczne udostępnienie danych (np. poprzez zastosowanie odpowiednich mechanizmów kryptograficznych).

15. Bezpieczeństwo przetwarzania danych osobowych

1) Nadleśnictwo wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa w odniesieniu do wyników analizy ryzyka (analizę ryzyka przeprowadza IOD) w tym między innymi w stosownych przypadkach wdraża:
   a) Pseudominizację i szyfrowanie danych;
   b) Zdolność zapewnienia stałej poufności, integralności i dostępności systemów i usług przetwarzania;
   c) Możliwość przywrócenia dostępu do danych osobowych w odpowiednim czasie, w przypadku wystąpienia incydentu technicznego lub fizycznego;
   d) Proces regularnego testowania i oceny skuteczności środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania danych.

2) Wyniki analizy ryzyka na podstawie, których wdraża się odpowiednie środki techniczne i organizacyjne są przekazywane przez Administratora danych Podmiotom przetwarzającym dane w celu zagwarantowania odpowiedniego poziomu bezpieczeństwa.

16. Audyty

1) Nadleśnictwo. przeprowadza systematyczne audyty stanu ochrony danych osobowych.
2) Audyty maja charakter planowy i pozaplanowy (doraźny).
3) Plan audytu jest przygotowany przez IOD na określony przez niego okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan jest przedstawiony Administratorowi Danych nie później niż na miesiąc przed rozpoczęciem okresu objętego planem. Plan audytu obejmuje co najmniej jedno sprawozdanie, zagadnienie (proces, zbiór, obiekt).
4) Audyt pozaplanowy jest przeprowadzony niezwłocznie po powzięciu przez IOD informacji o naruszeniu ochrony danych osobowych lub w uzasadnionym podejrzeniu takiego naruszenia. IOD informuje Administratora Danych o rozpoczęciu audytu poza planowanego przed podjęciem pierwszej czynności w toku sprawdzenia.
5) Administrator Danych przyjmuje od IOD do wiadomości plan audytów, a w przypadku audyty pozaplanowego (doraźnego), informację o rozpoczęciu takiego procesu.
6) Przed każdym audytem, IOD sporządza program sprawdzenia, w którym określa zakres czynności oraz sposób i zakres dokumentowania czynności sprawdzających.

7) IOD, może wystąpić o wydanie opinii przez osobę posiadającą wiedzę specjalistyczną, niezbędną do zapewnienia prawidłowości przeprowadzonego audytu (np. administratora systemu IT).
8) IOD zawiadamia Kierownika jednostki/Komórki organizacyjnej objętej audytem o zakresie czynności podlegających sprawdzeniu w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.
9) Kierownik jednostki/komórki organizacyjnej objęty sprawdzeniem bierze udział w czynnościach sprawdzających lub umożliwia IOD ich przeprowadzenie.
10) Obowiązku zawiadamiania kierownika jednostki/komórki organizacyjnej nie stosuje się w przypadku: audytu pozaplanowego, jeżeli niezbędne jest przywrócenie stanu zgodnego z prawem lub weryfikacji czy naruszenie miało miejsce.
11) Po zakończeniu audytu IOD przygotowuje raport i przekazuje administratorowi danych w terminach.
12) Raporty z audytów oraz dokumenty pomocnicze IOD przechowuje przez okres co najmniej pięciu lat od dnia ich sporządzenia.

17. Zasady obowiązujące przy zbieraniu danych osobowych w postaci nowych zbiorów danych

1) W sytuacji, gdy konieczne jest zebranie danych osobowych i utworzenie z nich nowego zbioru danych, kierownik jednostki/komórki organizacyjnej kieruje wniosek do Administratora danych, który podejmuje decyzję w sprawie utworzenia nowego zbioru danych osobowych.
2) Przed złożeniem wniosku u Administratora danych kierownik jednostki/komórki organizacyjnej uzyskuje opinię IOD w sprawie możliwości oraz prawidłowości zbierania danych osobowych w celu utworzenia nowego zbioru.
3) Wniosek kierowany do IOD zawierać powinien następujące informacje:
    a) proponowana nazwę zbioru,
    b) od kogo będą pozyskiwane dane osobowe,
    c) zakres danych jakie będą zbierane,
    d) cel zbierania danych osobowych,
    e) podmiot (jednostka bądź komórka organizacyjna) odpowiedzialna za gromadzone dane,
    f) informację o zamiarze lub powierzeniu do przetwarzania danych osobowych,
    g) forma prowadzenia zbioru (papierowa, elektroniczna lub papierowa i elektroniczna,
    h) wykaz stosowanych środków i mechanizmów zabezpieczeń,
    i) wykaz Systemów informatycznych służących do przetwarzania danych osobowych.
4) Opinia jest wydawana przez IOD w terminie nie dłuższym niż 14 dni od daty otrzymania Wniosku.

18. Przeglądy

Zasady ochrony danych osobowych podlegają regularnym przeglądom.

19. Dokumenty powiązane i załączniki

1) Załączniki
   a) Załącznik 1 - Umowa powierzenia przetwarzania danych- wzór.
   b) Załącznik 2 - Rejestr czynności przetwarzania – administrator danych – wzór.
   c) Załącznik 3 - Rejestr kategorii czynności przetwarzania – podmiot przetwarzający – wzór.
   d) Załącznik 4 - Procedura odbierania oświadczeń zgody na przetwarzanie danych osobowych.
   e) Załącznik 5 - Procedura realizacji praw osób, których dane dotyczą.
   f) Załącznik 6 - Upoważnienie do przetwarzania danych osobowych; Oświadczenie upoważnionego – wzór.
   g) Załącznik 7 - Ewidencja osób upoważnionych do przetwarzania danych osobowych – wzór.
   h) Załącznik 8 – Rejestr naruszeń.
   i) Załącznik 9 – Instrukcja zarządzania systemem informatycznym.

Załącznik nr 1.

Umowa Nr ……..
Powierzenia przetwarzania danych osobowych

Zawarta w dniu …… r. pomiędzy:
……,
……
……
reprezentowanym przez
……
zwanym w dalszej
Zleceniodawcą
a
……,
……
……
reprezentowanym przez
……

zwanym w dalszej
Zleceniobiorcą

Definicje

1. Dla potrzeb niniejszej umowy, o ile z treści i celu umowy nie wynika inaczej, przyjmuje

się następujące znaczenie dla poniżej wymienionych sformułowań:

1) „Umowa" – umowa na ……
2) „Dane osobowe" – dane osobowe w rozumieniu art. 4 RODO.
3) „Polityki"-polityka ochrony danych w rozumieniu RODO preambuła motyw 78.
4) „Zabezpieczenie danych osobowych"- oznacza zabezpieczenie danych osobowych w rozumieniu RODO art. 32, preambuła motyw 78.
5) „IOD" – Inspektor Ochrony Danych w rozumieniu RODO art. 37-39, preambuła motyw 97.
6) „Administrator" – Administrator Danych Osobowych w rozumieniu RODO art. 4.

2. Zleceniodawca oświadcza, że jest administratorem zbiorów danych osobowych.

3. Zleceniobiorca może przetwarzać dane osobowe powierzone do przetwarzania przez Zleceniodawcę w zakresie i celu zgodnym z Umową w zakresie :

4. Powierzenie przetwarzania danych osobowych nastąpi w okresie …….. miesięcy od dnia zawarcia Umowy.

5. Oświadczenia i obowiązki:

1) Zleceniobiorca niniejszym oświadcza i gwarantuje, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany Personel, w zakresie umożliwiającym należyte wykonanie Umowy powierzenia zgodnie z powszechnie obowiązującymi przepisami prawa na terytorium Polski. W szczególności Zleceniobiorca oświadcza i gwarantuje, że zna i stosuje zasady ochrony Danych osobowych wynikające z RODO;
2) Zleceniobiorca zobowiązuje się w szczególności
   a. przetwarzać Dane osobowe wyłącznie w zakresie określonym w Umowie powierzenia i wyłącznie celu należytego wykonania Umowy;
   b. przetwarzać Dane osobowe wyłącznie na udokumentowane polecenie Administratora danych (tj. przekazane w formie instrukcji, lub w innym pisemnym lub elektronicznym dokumencie dostarczonym przez Administratora), chyba że obowiązek taki nakłada na niego obowiązujące prawo unijne lub krajowe – w takim przypadku Zleceniobiorca informuje Administratora danych drogą elektroniczną na adres email _____ – przed rozpoczęciem przetwarzania – o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
   c. posługiwać się przy wykonywaniu Umowy powierzenia jedynie osobami, którym zostało udzielone imienne upoważnienie do przetwarzania danych w formie pisemnej;
   d. zobowiązać, w formie pisemnej, osoby, którymi posługuje się przy wykonywaniu Umowy powierzenia do zachowania Danych osobowych w tajemnicy;

e. wspierać Administratora danych, w szczególności poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO (Prawa osoby, której dane dotyczą). Wsparcie Zleceniobiorca powinno odbywać się w formie i terminie umożliwiającym należytą i terminową realizację takich obowiązków przez Administratora danych. Wobec powyższego Zleceniobiorca jest w szczególności zobowiązana do:

- udzielania informacji oraz ujawnienia Danych osobowych na żądanie Administratora danych w terminie 3 Dni Roboczych w formie określonej przez Administratora danych;
- Zleceniobiorca niezwłocznie, jednak nie później niż w terminie 3 Dni Roboczych, poinformować Administratora danych o wniosku dotyczącym realizacji praw osoby, której dane dotyczą, złożonym u Zleceniobiorcy; w celu uniknięcia wszelkich wątpliwości Zleceniobiorca nie będzie jednak odpowiadał na taki wniosek bez uprzedniej zgody lub wyraźnego polecenia Administratora danych;

f. pomagać Administratorowi danych wywiązać się z obowiązków określonych w RODO, a w szczególności tych wskazanych w art. 32-36 RODO), tj. w szczególności w zakresie:

- zapewnienia bezpieczeństwa przetwarzania Danych osobowych poprzez wdrożenie stosownych środków technicznych oraz organizacyjnych zgodnie z § 3 Umowy powierzenia;
- procedury zgłaszania naruszeń ochrony Danych osobowych organowi nadzorczemu oraz zawiadamiania osób, których dane dotyczą o takim naruszeniu, zgodnie z § 4 Umowy powierzenia;
- dokonywania przez Administratora danych oceny skutków dla ochrony danych oraz przeprowadzania konsultacji Administratora danych z organem nadzorczym;

g. prowadzić w formie pisemnej rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora danych, zgodnie z art. 30 RODO;

h. współpracować z Administratorem danych w razie prowadzenia kontroli, audytu czy inspekcji w zakresie przetwarzania Danych osobowych przez uprawniony organ lub w związku z prowadzonym przez Administratora danych audytem;

i. przekazywać Administratorowi danych kopie protokołów kontroli, wystąpień lub stanowisk organów, skierowanych do Zleceniobiorca, bez odrębnego wezwania Administratora danych, nie później niż w ciągu 3 Dni Roboczych od dnia ich otrzymania;

j. niezwłocznie informować Administratora danych, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów unijnych lub krajowych o ochronie danych. Zleceniobiorca przekazuje taką informację w formie elektronicznej na adres e-mail ……., a informacja ta powinna zawierać w szczególności: 1) wskazanie przepisu, który narusza wydane polecenie oraz 2) uzasadnienie zawierające argumenty natury faktycznej i prawnej

3) Zleceniobiorca uznaje obowiązek ochrony danych osobowych za obowiązek wszystkich swoich pracowników, niezależnie od stosunku prawnego łączącego Zleceniobiorca z powyższymi osobami. Jednocześnie zobowiązuje się, że w przypadku, gdy którakolwiek z osób wskazanych w zdaniu poprzednim naruszy jakikolwiek zasady przestrzegania ochrony danych osobowych, niezwłocznie odsunie ją od wykonywania czynności związanych z Umową powierzenia oraz uniemożliwi jej dostęp do jakichkolwiek Danych osobowych Administratora.

4) ZLECENIOBIORCA zobowiązuje się wdrożyć i stosować odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których Dane osobowe będą przetwarzane na podstawie Umowy powierzenia oraz zapewnia realizację zasad ochrony danych w fazie projektowania (*privacy by design*) oraz domyślnej ochrony danych (*privacy by default*) - art. 25 RODO. Zleceniobiorca jest zobowiązana wdrożyć odpowiednie środki techniczne i organizacyjne.

5) Administrator danych ma prawo wydawać Zleceniobiorcy wiążące instrukcje dotyczące wdrożenia dodatkowych/nowych środków zabezpieczających. Zleceniobiorca powinna wdrożyć takie środki w terminie uprzednio uzgodnionym z Administratorem danych.

6. Obowiązki informacyjne i Incydenty

1) Zleceniobiorca zobowiązana jest niezwłocznie, jednakże nie później niż w ciągu 2 Dni Roboczych (48 godzin) od dnia powzięcia informacji, zawiadomić Administratora danych na adres e-mail:…….. o:

a. prowadzonej lub planowanej kontroli, audycie czy inspekcji w zakresie przetwarzania Danych osobowych oraz umożliwić Administratorowi danych udział w tej kontroli, audycie czy inspekcji, o ile nie sprzeciwiają się temu przepisy prawa bezwzględnie obowiązującego ani organ prowadzący kontrolę;

b. wszelkich czynnościach z własnym udziałem w sprawach dotyczących ochrony Danych osobowych prowadzonych przez organy administracji państwowej lub samorządowej, w tym w szczególności przez krajowy organ nadzoru (w tym w szczególności wszelkiej korespondencji z GIODO, UODO lub innym organem nadzorczym z ww. organami, decyzjach przez nie wydanych, rozpatrywanych skarg, prowadzonych lub zapowiedzianych kontrolach), Policję lub sąd (w tym w szczególności wszelkich

postępowaniach, których przedmiotem byłoby powierzenie w przetwarzanie Danych osobowych), chyba że będzie to sprzeczne z decyzją wydaną przez organy administracji publicznej lub z przepisami prawa – o których posiada wiedzę.

7. Zleceniobiorca zobowiązana jest niezwłocznie, nie później jednak niż w ciągu 12 godzin, zawiadomić Administratora danych o każdym zaistniałym incydencie (dalej jako: „**Incydent**") przez który rozumie się:

1) naruszenie zasad ochrony Danych osobowych lub
2) podejrzenie naruszenia lub
3) próbę naruszenia zasad ochrony Danych osobowych.

a. Zgłoszenie Incydentu powinno zostać dokonane drogą telefoniczną pod nr …… oraz jednocześnie na adres e-mail: ……. i zawierać co najmniej następujące informacje:

a) szczegółowy opis Incydentu, a w szczególności datę, czas trwania, miejsce wystąpienia Incydentu i jego skalę (m.in. przybliżona liczba osób, których dotyczy Incydent oraz kategorie tych osób);

b) imię i nazwisko oraz dane kontaktowe do osoby, mogącej udzielić dalszych informacji o Incydencie;

c) opis zastosowanych środków w celu zminimalizowania ewentualnych negatywnych skutków Incydentu.

b. Zleceniobiorca zobowiązana jest niezwłocznie, jednakże nie później jednak niż w ciągu 12 godzin przekazać Administratorowi danych wszelkie dokumenty i informacje związane z Incydentem na każde żądanie Administratora danych.

c. Zleceniobiorca zobowiązana jest zastosować się do wszelkich wytycznych lub poleceń Administratora danych w celu zminimalizowania ewentualnych negatywnych skutków Incydentu i zapobiegnięcia jego powtórzeniu w przyszłości.

8. Usunięcie Danych osobowych:

1) Nie później niż w ciągu 30 dni od dnia wygaśnięcia lub rozwiązania Umowy, Zleceniobiorca zobowiązuje się:

a. komisyjnie zniszczyć wszelkie nośniki Danych osobowych (w tym wszelkie kopie Danych osobowych, w tym kopie robocze i archiwalne) oraz doręczyć Administratorowi danych pisemne oświadczenie (forma pisemna pod rygorem nieważności) o ich zniszczeniu podpisane przez Zleceniobiorca oraz wszystkich członków komisji, którzy uczestniczyli w zniszczeniu albo

b. zwrócić Administratorowi danych w/w nośniki Danych osobowych

- w zależności od żądania Administratora danych, złożonego Zleceniobiorcy za pomocą poczty elektronicznej na adres email _____ - z uwzględnieniem ust. 2 poniżej.

Oświadczenie o zniszczeniu nośników zostanie przesłane w formie skanu podpisanego dokumentu na adres email:……, a oryginał, w terminie 3 Dni Roboczych od dnia zniszczenia nośników Danych osobowych, wyśle listem poleconym lub doręczy osobiście na adres: …….. .

a) W celu uniknięcia wątpliwości Strony zgodnie oświadczają, że w przypadku Danych osobowych zapisanych w infrastrukturze informatycznej, takiej jak serwery, komputery, nośniki pamięci masowej lub inny sprzęt komputerowy, Administrator danych nie jest uprawniony do żądania wydania mu elementów infrastruktury informatycznej, o której mowa powyżej, w których zostały zapisane Dane osobowe. Dane osobowe zapisane w infrastrukturze informatycznej zostaną w takim wypadku trwale zniszczone (usunięte), bez możliwości ich odtworzenia (przywrócenia) w jakikolwiek sposób.

9. Zmiana niniejszej umowy powierzenia może nastąpić tylko w formie pisemnej pod rygorem nieważności.

10. W sprawach nieuregulowanych niniejszą umową powierzenia mają zastosowania przepisy obowiązującego prawa.

11. Umowa wchodzi w życie z dniem jej zawarcia.

12. Niniejszą umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Administrator/Zleceniodawca Zleceniobiorca

Załącznik nr 2

Rejestr czynności przetwarzania

Nazwa i dane kontaktowe administratora	
Nazwa	Nadleśnictwo Ciechanów
Adres	ul. Płocka 21c, 06-400 Ciechanów
Email	ciechanow@olsztyn.lasy.gov.pl
Telefon	23 672 45 16

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	Formica Szerszenowicz Sp Jawna. - wyznaczony pracownik Rafał Nalewajko
Adres	ul.Gruntowa 9/1 lok. 102; 15-706 Białystok
Email	ciechanow@iod.expert; rafal.nalewajko@formica.com.pl
Telefon	85 7444 000; 668 028 173

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

Załącznik nr 2.

LP.	Zbiór	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział, stanowisko itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
				Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Rekrutacja, pracownicy i współpracownicy.	**Rekrutacja pracowników**	Stanowisko ds. pracowniczych	Rekrutacja pracowników	Kandydaci do pracy	imię nazwisko, adres email, numer telefonu, dane kontaktowe, dane o wykształceniu, uprawnienia zawodowe, doświadczenie zawodowe, posiadanie prawa jazdy	• Zgoda osób, których dane dotyczą	Kandydaci do pracy	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Nie dotyczy	nie dotyczy		Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych, niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
2		**Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy**	Stanowisko ds. pracowniczych	Prowadzenie ewidencji pracowników zgodnie z Kodeksem pracy	Pracownicy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem pracy , stopień niepełnosprawności• Imiona i nazwisko • Nazwisko rodowe • Imiona rodziców • Nazwisko rodowe matki • Adres zamieszkania • PESEL • NIP • Data urodzenia • Miejsce urodzenia • Seria i numer dowodu osobistego, organ wydający, data wydania oraz data ważności • Powszechny obowiązek obrony • Obywatelstwo • Przebieg pracy zawodowej • Informacje dotyczące wykształcenia • Członkowie rodziny • Dane osoby, którą należy zawiadomić w razie wypadku • Numer rachunku bankowego • Informacja na temat karalności	• Umowa o pracę • Przepis prawa Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2018 r., poz. 108) - w szczeg. art. 22^1 w związku z art. 94 pkt 9a i 9b Ustawa z dnia 28 września 1991 o lasach (t.j. Dz. U. z 2017 r., poz. 788)	Pracownik	50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe, ubezpieczenia grupowe, medycyna pracy	Płatnik, SIlP, Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
3		**Zgłoszenie pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach**	Dział finansowo-księgowy	Zgłoszenia pracownika i członków jego rodziny do ZUS, aktualizacja zgłoszenia oraz przekazywanie informacji o zwolnieniach	Pracownicy i członkowie rodzin, osoby uposażone	Dane identyfikacyjne, dane adresowe, dane o Odziale Kasy Chorych oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA - zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny	• Przepis prawa. Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a	Pracownik	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Płatnik, SIlP, Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych, niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
4		**Prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS**	Dział finansowo-księgowy	Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS	Pracownicy	Dane identyfikacyjne, dane adresowe, dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach (składki związkowe, zajęcia komornicze itp.), numery kont dla przelewów bankowych pracownika	Umowa o pracę. Przepis prawa. • Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 108 t.j.) Dział III - Wynagrodzenia; ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a;	Pracownik	50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]	Nie dotyczy	Nie dotyczy	Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Płatnik, SIlP, Dokumentacja papierowa.	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
5		**Przetwarzanie danych w ramach Zakładowego Funduszu Świadczeń Socjalnych**	Dział administracyjno-gospodarczy, Komisja Socjalna	Ustalenie poziomu świadczeń. Zawiera dane osób ubiegających się o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych.	Pracownicy	• nazwiska i imiona, • adres zamieszkania lub pobytu, • oświadczenie o osiąganiu dochodu	• Ustawa z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych t.j. Dz. U. z 2017 r. poz. 2191, 2371.	Pracownik	5 lat	Nie dotyczy	Nie dotyczy	brak	Forma papierowa	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
6		**Korzystanie przez pracowników z dodatkowych benefitów (kart sportowych, ubezpieczenia, opieki medycznej)**	Dział administracyjno-gospodarczy, Komisja Socjalna	udzielanie dodatkowy świadczeń na rzecz pracowników i ich rodzin	Pracownicy i członkowie rodzin, osoby uposażone	• nazwiska i imiona, dane kontaktowe	zgoda	pracownik	5 lat	Nie dotyczy	Nie dotyczy	Medycyna pracy, Dostawcy kart lojalnościowych, opieka medyczna, ubezpieczyciele	Forma papierowa, forma elektroniczna, system ERU	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
7		**Wykorzystywanie wizerunku pracowników**	Stanowisko ds. pracowniczych, Dział gospodarki leśnej	W celach informacyjnych i marketingowych	pracownicy	imię i nazwisko oraz wizerunk	zgoda	pracownik	do zakończenia zatrudnienia	Nie dotyczy	Nie dotyczy	podmioty świadczące usługi w zakresie marketingu, drukowania i publikacji materiałów	Forma papierowa, forma elektroniczna	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
8		**Podnoszenie kwalifikacji i szkolenia pracowników**	Stanowisko ds. pracowniczych	Szkolenia pracowników	pracownicy	imię nazwisko, data urodzenia,	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 108 t.j.) art. 100 § 1	pracownik	50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy	Nie dotyczy	podmioty świadczące usługi szkoleniowe	Forma papierowa, forma elektroniczna	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
9		**Prowadzenie postepowań w trybie zamówień publicznych**	Dział administracyjno-gospodarczy; Dział gospodarki leśnej														
10		**Nawiązywanie współpracy**	Dział administracyjno-gospodarczy; Dział gospodarki leśnej	Sprzedaż produktów	kontrahenci	dane firm, dane kontaktowe pracowników, adresy email,	zgoda, umowa	działania handlowe, marketing,	5 lat po zakończeniu współpracy	Nie dotyczy	Nie dotyczy		oprogramowanie pocztowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.			
11		**Realizacja umów**	Dział Gospodarki Leśnej	Sprzedaż produktów	kontrahenci, klienci końcowi	dane firm, dane kontaktowe pracowników, adresy email,	umowa	klienci	5 lat po zakończeniu współpracy	Nie dotyczy	Nie dotyczy		oprogramowanie pocztowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.			

LP.	Zbiór	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział, stanowisko itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
				Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
12	Klienci	**Sprzedaż**	Dział Gospodarki Leśnej	Sprzedaż produktów	kontrahenci, klienci końcowi	dane firm, dane kontaktowe pracowników adresy email, dane kierowców, imie, nazwisko, numer dokumentu. Cel – weryfikacja osoby zgłaszającej się pod załadunek	umowa	klienci	5 lat po zakończeniu współpracy	Nie dotyczy	Nie dotyczy		oprogramowanie pocztowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
13		**Polowania**	Dział Gospodarki Leśnej	obsługa polowań, prowadzenie książka ewidencji pobytu na polowaniu indywidualnym	myśliwi	imię i nazwisko myśliwego, numer upoważnienia do wykonywania polowania indywidualnego	Ustawa z dnia 13 października 1995 r. Prawo łowieckie (t.j. Dz.U. z 2017 r. poz. 1295, z 2018 r. poz.50, 650, 651.)		zgodnie z instrukcją kancelaryjną	Nie dotyczy		rejestr jawny		zamykane szafy, upoważnienia,	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
14		**Odszkodowania łowieckie**	Dział Gospodarki Leśnej	szacowanie szkód i ustalanie wysokości odszkodowania	właściciele albo posiadacze gruntów rolnych	imię i nazwisko albo nazwę, adres miejsca zamieszkania albo adres i siedzibę oraz numer telefonu właściciela albo posiadacza gruntów rolnych	Ustawa z dnia 13 października 1995 r. Prawo łowieckie (t.j. Dz.U. z 2017 r. poz. 1295, z 2018 r. poz.50, 650, 651.)		zgodnie z instrukcją kancelaryjną	Nie dotyczy				Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
15		**Reklamacje**	Dział Gospodarki Leśnej	Realizacja zobowiązań gwarancyjnych	kontrahenci, klienci końcowi	dane firm, imię nazwisko, adresy email, telefon kontaktowy, dane dotyczące pojazdu, numer VIN, numer rejestracyjny, dane kierowców, imie, nazwisko, numer dokumentu. Cel – weryfikacja osoby zgłaszającej się pod załadunek	umowa	klienci	5 lat	Nie dotyczy	Nie dotyczy		oprogramowanie pocztowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
16		**Przyjmowanie skarg i wniosków**	Kancelaria Nadleśnictwa (sekretariat)	rozpatrywanie spraw zwiazanych ze złożonymi skargami i wnioskami	kontrahenci, klienci końcowi, podmioty zewnętrzne, urzędy	dane firm, imię nazwisko, adresy email, telefon kontaktowy, numer IP komputera, dane pracowników w zakresie składanych pism	art. 63 Konstytucji RP (Dz.U z 1997 r. Nr 78, poz. 483); Dział VIII kodeksu postępowania administracyjnego (tekst jedn. Dz.U. 2017 poz. 1257); rozporządzenie Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków (Dz.U z 2002 r. Nr 5, poz. 46).	osoby, których dane dotycza, osoby trzecie	zgodnie z instrukcją kancelaryjną	Nie dotyczy		podmioty biorące udział w postepowaniu	oprogramowanie pocztowe	Wszelkie dane są zabezpieczone i przechowywane w szafie pod kluczem, w wersji elektronicznej hasłem, niszczarki dokumentów	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
17		**Prowadzenie rejestru korespondencji**	Kancelaria Nadleśnictwa (sekretariat)	Prowadzenie ewidencji korespondencji oraz odbiór i wysyłanie korespondencji	kontrahenci, klienci końcowi, podmioty zewnętrzne, urzędy	dane firm, imię nazwisko, adresy email, telefon kontaktowy, numer IP komputera, dane pracowników w zakresie składanych pism		podmioty danych	5 lat	Nie dotyczy	Nie dotyczy	firmy niszczące dokumenty	oprogramowanie pocztowe	Wszelkie dane są zabezpieczone i przechowywane w szafie pod kluczem, w wersji elektronicznej hasłem, niszczarki dokumentów	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
18	Straż leśna	**Dochodzenie**	Posterunek straży leśnej	Dane osobowe gromadzone w tym zbiorze zbierane są w wyniku podejrzenia o popełnienie przestępstwa (szkoda leśna).	osób podejrzanych o popełnienie wykroczenia lub przestępstwa oraz świadkowie	• Imiona i nazwisko • Cechy dowodu osobistego lub innego dokumentu stwierdzającego tożsamość • PESEL • Pseudonim • Nazwisko rodowe • Imiona rodziców • Nazwisko rodowe matki • Data urodzenia • Miejsce urodzenia • Miejsce zameldowania na pobyt stały • Miejsce zamieszkania • Adres korespondencyjny • Obywatelstwo • Wykształcenie • Stan cywilny • Liczba dzieci i ich wiek • Liczba osób na utrzymaniu i sposób pokrewieństwa • Stan zdrowia • Zawód wyuczony • Miejsce pracy lub źródło utrzymania • Zajmowane stanowisko służbowe lub wykonywane czynności • Uposażenie lub zarobki • Stan majątkowy • Służba wojskowa • Ordery i odznaczenia	ustawa z dnia 28 września 1991 r. o lasach (Dz. U. z 2015, poz. 2100) oraz ustawy z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (t.j. Dz. U. z 2018 r. poz. 424, 730.)	Dane osobowe przetwarzane w tym zbiorze pochodzą bezpośrednio od osób podejrzanych o popełnienie wykroczenia lub przestępstwa oraz od świadków	ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (t.j. Dz. U. z 2018 r. poz. 424, 730.) art.. 14 - 15 lat				Dane przetwarzane są w formie kartotek papierowych (protokoły przesłuchań, książka służbowa strażnika leśnego, repertorium, ewidencja zgłoszeń szkód leśnych)	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
19		**Nakładanie mandatów i pouczanie**	Posterunek straży leśnej	Dane osobowe gromadzone w tym zbiorze zbierane są w wyniku podejrzenia o popełnienie przestępstwa (szkoda leśna).	osób podejrzanych o popełnienie wykroczenia lub przestępstwa oraz świadkowie	• Imię i nazwisko • Nr dowodu osobistego • PESEL • Adres zamieszkania lub pobytu	ustawa z dnia 28 września 1991 r. o lasach (Dz. U. z 2015, poz. 2100) oraz ustawy z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (t.j. Dz. U. z 2018 r. poz. 424, 730.)	Dane osobowe przetwarzane w tym zbiorze pochodzą bezpośrednio od osób podejrzanych o popełnienie wykroczenia lub przestępstwa oraz od świadków	ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (t.j. Dz. U. z 2018 r. poz. 424, 730.) art.. 14 - 15 lat			Policja	Dane przetwarzane są w formie kartotek papierowych (protokoły przesłuchań, książka służbowa strażnika leśnego, repertorium, ewidencja zgłoszeń szkód leśnych)	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy
20		**Monitoring wizyjny**	Dział Administracyjno-Gospodarczy; administratorzy SILP	Ochrona osób i mienia	Dane z tego zbioru pochodzą z kamer monitoringu wizyjnego obejmującego wnętrze budynku Nadleśnictwa oraz bezpośrednie otoczenie.	. Dane dotyczę wizerunku osób przebywających w monitorowanych obszarze · Numery rejestracyjne pojazdów przebywających w monitorowanych obszarze	Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust. 1 lit. f) RODO).	podmiot danych	3 miesiące		Firma ochroniarska	Policja	system monitoringu wizyjnego	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych. Niszczarki dokumentów.	Brak - DPIA nie jest wymagane	Nie dotyczy	Nie dotyczy

***Kolorem czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO**

brak monitoringu
brak ohz
brak polowań
brak odszkodowań

Załącznik nr. 3

Rejestr kategorii czynności przetwarzania

	Nazwa i dane kontaktowe administratora
Nazwa	Nadleśnictwo Ciechanów
Adres	ul. Płocka 21c, 06-400 Ciechanów
Email	ciechanow@olsztyn.lasy.gov.pl
Telefon	23 672 45 16

	Inspektor Ochrony Danych (jeśli powołano)
Nazwa	Formica Szerszenowicz Sp Jawna. - wyznaczony pracownik Rafał Nalewajko
Adres	ul.Gruntowa 9/1 lok. 102; 15-706 Białystok
Email	ciechanow@iod.expert; rafal.nalewajko@formica.com.pl
Telefon	85 7444 000; 668 028 173

	Przedstawiciel (jeśli wyznaczono)
Nazwa	
Adres	
Email	
Telefon	

Załącznik nr. 3

LP.	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania					Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
			Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)		numer umowy	czas reakcji w przypadku naruszenia	informacja o postępowaniu organu kontrolnego, sądowym lub administracyjnym	planowanie audytu (informacja przed podjęciem audytu przez Administratora)			Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań
LP.	1	2	3	4	5	6	7					8	9	10	11
	Art. 30 ust. 2 lit. b	Art. 30 ust. 2 lit. d, art. 32 ust. 1	Art. 30 ust. 2 lit. a									Art. 30 ust. 2 lit. c	Art. 30 ust. 2 lit. c		
1	Realizacja świadczeń na rzecz pracowników	Kontrola dostępu do infrastruktury, aplikacji i baz danych wg. ustalonych uprawnień Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze). Szyfrowana transmisja danych Zamykane pomieszczenia Zamykane szafy Niszczarki dokumentów Wdrożone rozwiązania informatyczne w postaci oprogramowania antywirusowego zabezpieczającego stacje robocze i serwery	Medicover Forsakring AB (publ.) Spółka Akcyjna - Oddział w Polsce	nie dotyczy	nie dotyczy	IOD_INS@medicover.pl	realizacja usług w zakresie korzyści pracowniczych	porozumienie do umowy z dnia 09.10.2017				nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
2	Realizacja świadczeń na rzecz pracowników	Kontrola dostępu do infrastruktury, aplikacji i baz danych wg. ustalonych uprawnień Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze). Szyfrowana transmisja danych Zamykane pomieszczenia Zamykane szafy Niszczarki dokumentów Wdrożone rozwiązania informatyczne w postaci oprogramowania antywirusowego zabezpieczającego stacje robocze i serwery	Medicover Sp. z .o.o.	nie dotyczy	nie dotyczy	IOD@medicover.pl	realizacja usług w zakresie korzyści pracowniczych	brak				nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy
3	Realizacja świadczeń na rzecz pracowników	Kontrola dostępu do infrastruktury, aplikacji i baz danych wg. ustalonych uprawnień Dostęp do danych otrzymują wyłącznie osoby wskazane przez przetwarzającego na zlecenie administratora (czynności związane z modyfikacją funckjonalności, konserwacyjne, naprawcze). Szyfrowana transmisja danych Zamykane pomieszczenia Zamykane szafy Niszczarki dokumentów Wdrożone rozwiązania informatyczne w postaci oprogramowania antywirusowego zabezpieczającego stacje robocze i serwery	PZU SA, al. Jana Pawła II 24, 00-133 Warszawa	nie dotyczy	IODpzu@pzu.pl	IODpzu@pzu.pl	świadczenie ubezpieczeń zdrowotnych pracownikom przez PZU Życie S.A.	z dnia 15 maja nr 241306103	24 godziny	48 godzin		nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy

Załącznik nr 4.

Procedura odbierania oświadczeń zgody na przetwarzanie danych osobowych

1. Cel procedury

Celem procedury jest określenie zasad odbierania oświadczeń woli od osób, których dane dotyczą o zgodzie na przetwarzanie ich danych osobowych.

2. Podstawa prawna

Zasady przedstawione w Procedurze zostały oparte na wymaganiach Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

3. Przebieg procesu

1) Odbieranie oświadczeń zgody na przetwarzanie danych osobowych

a) We wszystkich przypadkach, w których jedyną podstawą do przetwarzania danych osobowych, jest zgoda osoby, której dane dotyczą odbiera się taką zgodę w sposób sformalizowany i możliwy do udowodnienia.
b) Kierownik jednostki/komórki organizacyjnej jest zobowiązany do uzyskania opinii IOD w zakresie obowiązku pozyskania zgody na przetwarzanie danych osobowych w momencie wystąpienia nowego celu i/lub zakresu ich przetwarzania.
c) Klauzulę zgody przygotowuje IOD na podstawie informacji określonych w pkt b).
d) Za zamieszczenie klauzuli zgody oraz skuteczne jej pobranie od osoby, której dane dotyczą odpowiedzialny jest Kierownik jednostki/komórki organizacyjnej przetwarzającej te dane w konkretnym celu.
e) Zgoda musi być przedstawiona w jasny i zrozumiały dla odbiorcy sposób wskazując na konkretny cel przetwarzania, musi być wyodrębniona i wyszczególniona od pozostałej treści.
f) Zgoda nie może być wymuszona. Nie może być od niej uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.
g) W przypadkach, gdy jest to podyktowane wykorzystaniem technologii informatycznych zgoda może być wyrażona w sposób elektroniczny, należy przy tym pamiętać, że Nadleśnictwo zobowiązane jest do udowodnienia, że konkretna zgoda została wyrażona w sposób zgody z powszechnie obowiązującymi przepisami prawa.

2) Warunki wyrażenia zgody przez dziecko

a) Zakres świadczonych usług co do zasady wyklucza możliwość zbierania danych osobowych osoby poniżej 13 roku życia, dlatego tam, gdzie jest to możliwe należy wdrożyć mechanizmy weryfikujące wiek osoby, której dane dotyczą.
b) W przypadku zbierania danych osobowych od osób poniżej 16 roku życia należy pobrać zgodę od jej rodzica lub opiekuna, bądź aprobatę takiej osoby na uprzednio wyrażoną zgodę osoby poniżej 16 roku życia.
c) W każdym przypadku uniemożliwiającym stwierdzenie czy zgoda została zaaprobowana bądź wyrażona przez rodzica lub opiekuna należy zgodę uznać za niebyłą i zaprzestać, bądź nie rozpoczynać przetwarzania danych osoby, która nie ukończyła 16 roku życia.

1) Wycofanie zgody

a) Osoba, której dane przetwarzane są na podstawie zgody, ma prawo do jej cofnięcia w dowolnym momencie, o czym należy ją poinformować w momencie pobierania zgody.
b) Wycofanie zgody nie rodzi skutków wstecz.
c) Wycofanie zgody musi być równie łatwe jak jej wyrażenie i odbywać się każdym kanałem komunikacyjnym, w którym możliwe jest ustalenie tożsamości danej osoby.
d) Wycofanie zgody jest możliwe poprzez kanał komunikacyjny umożliwiający potwierdzenie tożsamości danej osoby.
e) Nie należy wymagać od osoby, której dane dotyczą szczególnej treści oświadczenia, a w przypadku jego ogólnego brzmienia należy przyjąć najszerszy możliwy zakres jego związania.

Załącznik nr 5.

Procedura realizacji praw osób, których dane dotyczą

1. Cel procedury

Celem procedury jest określenie sposobu realizacji praw osób, których dane dotyczą w sposób zgodny z przepisami powszechnie obowiązującego prawa o ochronie danych osobowych, a także zapewniający przejrzystość i rozliczalność.
Proces realizacji prawa osób, których dane dotyczą obejmuje:
- Prawo do bycia poinformowanym,
- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do usunięcia danych (bycia zapomnianym),
- Prawo do ograniczenia przetwarzania,
- Prawo do przenoszenia danych,
- Prawo do sprzeciwu,
- Prawo do wniesienia odwołania od zautomatyzowanego podejmowania decyzji.

Wyżej wymienione prawa osób, których dane dotyczą zostały wymienione w Rozdziale 9 Polityki ochrony danych.

2. Podstawa prawna

Zasady przedstawione w Procedurze zostały oparte na wymaganiach Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

3. Przebieg procesu

1) Prawo do bycia poinformowanym

a) We wszystkich przypadkach tego wymagających stosuje się klauzule informacyjne.
b) Do przypadków, w których niezbędne jest zastosowanie klauzuli informacyjnej zaliczyć należy:
   - pozyskiwanie CV w procesach rekrutacyjnych,
   - pozyskiwanie subskrybentów newslettera,
   - zbieranie danych klienta,
   - pozyskiwanie kontaktów do celów marketingowych,
   - wszelkie przypadki zbierania danych na podstawie zgody.
c) treści klauzuli informacyjnej decyduje IOD Administratora Danych, kierując się przy tym wymaganiami powszechnie obowiązującego prawa.

2) Prawo dostępu do danych

d) W każdym przypadku osoba, której dane dotyczą, może zwrócić się z wnioskiem o dostęp do danych jej dotyczących.
e) Wniosek powinien zawierać co najmniej imię i nazwisko oraz dane identyfikujące osobę, która składa dany wniosek.
f) Jeżeli zachodzi konieczność Administrator danych kontaktuje się z Wnioskodawcą w celu ustalenia operacji danych, w ramach których przetwarzanie mogło mieć miejsce.

g) Prawo dostępu realizowane jest w zależności od kategorii osoby, której dane dotyczą Osobą odpowiedzialną za prawidłową realizację danego wniosku jest IOD, do której został skierowany wniosek osoby, której dane dotyczą.
h) W celu prawidłowej realizacji prawa dostępu do danych na wniosek osoby, której dane dotyczą IOD przekazuje zapytanie do właściwych jednostek/komórek organizacyjnych Administratora Danych i Podmiotu Przetwarzającego o danej osobowe w zakresie:
   - celów przetwarzania,
   - kategoriach przetwarzanych danych osobowych,
   - informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
   - planowanego okresu przechowywania, dla każdego z celów przetwarzania, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   - źródła pochodzenia danych – w przypadku gdy nie zostały one zebrane od osoby, której dotyczą,
   - informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, jeżeli zachodzi.
i) Wyznaczone jednostki/komórki organizacyjnej, do których IOD skierował zapytanie mają 14 dni na odpowiedź na zapytanie IOD.
j) IOD jest odpowiedzialny za przygotowanie odpowiedzi w nieprzekraczalnym terminie 30 dni od dnia wpłynięcia wniosku. Jednocześnie IOD ma prawo scedować obowiązek przygotowania odpowiedzi na merytoryczną jednostkę/komórkę organizacyjną.
k) Odpowiedź musi zostać sporządzona w prostym i zrozumiałym języku i zaopatrzona dodatkowo informacjami o:
   - prawie do żądania od Administratora danych sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz wniesienia sprzeciwu wobec takiego przetwarzania,
   - prawie wniesienia skargi do organu nadzorczego,
   - o zasadach podejmowania zautomatyzowanych decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą oraz o prawie wniesienia odwołania do decyzji podjętej w taki sposób – w sytuacjach gdy zautomatyzowane podejmowanie decyzji występuje.
l) W przypadku wnioskowania o kopię danych podlegających przetwarzaniu załącza się tę kopie do odpowiedzi
m) IOD odnotowuje fakt udzielenia odpowiedzi na wniosek w rejestrze wraz z podaniem daty i sposobu przekazania odpowiedzi wraz z kopią wniosku i udzielonej odpowiedzi.

3) Prawo do sprostowania danych

a) Osoba, której dane dotyczą ma prawo wnioskowania o sprostowanie (korekta błędu) przetwarzanych przez Administratora danych jej danych osobowych, w tym do ich uzupełnienia jeżeli jest do niezbędne dla prawidłowego wykonania celu przetwarzania.
b) W każdym przypadku osoba, której dane dotyczą, ma prawo złożenia wniosku o sprostowanie jej danych.

c) Wniosek winien zawierać co najmniej imię i nazwisko oraz dane identyfikujące osobę, która go składa.

d) Jeżeli zachodzi konieczność Administrator danych kontaktuje się z Wnioskodawcą w celu ustalenia operacji danych, w ramach których przetwarzanie mogło mieć miejsce.

e) W przypadku uwzględnienia wniosku osoby, której dane dotyczą, IOD informuje właściwe jednostki/komórek organizacyjnych Administratora Danych i Podmiotu Przetwarzającego przetwarzające te dane o konieczności sprostowania danych osoby, która złożyła wniosek.

f) W terminie 7 dni Kierownicy jednostek/komórek organizacyjnych Administratora Danych i Podmiotu Przetwarzającego przekazują do IOD/ informację zwrotną o wykonaniu sprostowania danych osoby, której dane dotyczą.

g) IOD w ciągu 30 dni od daty wpłynięcia wniosku sporządza odpowiedź kierowana do osoby, której dane dotyczą. Jednocześnie IOD ma prawo scedować obowiązek przygotowania odpowiedzi na merytoryczną jednostkę/komórkę organizacyjną.

h) W przypadku odmowy uwzględnienia wniosku IOD wraz z informacją o jego odrzuceniu przesyła uzasadnienia napisane jasnym i prostym językiem.

i) IOD odnotowuje fakt dokonania sprostowania bądź przesłania informacji o odmowie sprostowania w rejestrze wskazując datę oraz formę odpowiedzi. wraz z kopią wniosku i udzielonej odpowiedzi.

4) Prawo do usunięcia danych

a) Nadleśnictwo uwzględniając wszelkie prawne aspekty gwarantują realizację prawa do usunięcia danych osobowych osoby, której dane dotyczą, a która zwróciła się z takim wnioskiem.

b) Bezwzględną przesłanką do usunięcia danych osobowych jest:

- cofnięcie zgody, na której przetwarzanie się opiera,
- dane osobowe stały się zbędne dla celu, w którym zostały zebrane, lub ustał ten cel,
- dane osobowe były przetwarzane niezgodnie z prawem.

c) Nadleśnictwo nie realizuje wniosku o usunięcie danych, gdy zachodzi podstawa prawna nakładająca na Administratora Danych obowiązek przetwarzania tych danych.

d) Wniosek winien zawierać co najmniej imię i nazwisko oraz dane identyfikujące, osobę która go składa.

e) Jeżeli zachodzi konieczność Administrator danych kontaktuje się z Wnioskodawcą w celu ustalenia operacji danych, w ramach których przetwarzanie mogło mieć miejsce.

f) IOD nadzoruje prawidłowość realizacji wniosku, poprzez zapytanie właściwe jednostki/komórki organizacyjne Administratora Danych czy nie istnieją przeciwskazania do realizacji przedmiotowego wniosku np. w związku z ciążącym na Administratorze danych obowiązku prawnym.

g) W terminie do 7 dni Kierownicy jednostek/komórek organizacyjnych Administratora Danych i informują IOD o możliwości realizacji wniosku. Na podstawie przedmiotowej informacji IOD zleca usunięcie danych bądź informuje

właściwą jednostkę/komórkę organizacyjną o odmowie uwzględnienia wniosku w części lub całości.

h) IOD w terminie 30 dni sporządza informację dla wnioskodawcy, a odmowę wykonania wniosku należy obowiązkowo zaopatrzyć uzasadnieniem napisanym jasnym i czytelnym językiem. Jednocześnie IOD ma prawo scedować obowiązek przygotowania odpowiedzi na merytoryczną jednostkę/komórkę organizacyjną.

i) IOD w rejestrze uwzględnienia fakt wniosku, bądź braku jego realizacji z podaniem daty i formy odpowiedzi wraz z kopią wniosku i udzielonej odpowiedzi.

5) Prawo do ograniczenia przetwarzania

a) Nadleśnictwo gwarantuje prawo do ograniczenia przetwarzania gdy jest to możliwe zgodnie z zasadami powszechnie obowiązującego prawa.

b) Wniosek o ograniczenie przetwarzania powinien zawierać imię i nazwisko oraz dane identyfikujące osobę składającą wniosek.

c) Jeżeli zachodzi konieczność Administrator danych kontaktuje się z Wnioskodawcą w celu ustalenia operacji danych, w ramach których przetwarzanie mogło mieć miejsce.

d) Dodatkowo wniosek powinien zawierać kategorie danych, których ograniczenie ma dotyczyć wraz z podaniem podstawy do ograniczenia przetwarzania.

e) Za prawidłowość wypełnienia obowiązku odpowiedzialny jest IOD, który w tym zakresie związany jest postanowieniami wniosku i powszechnie obowiązujących przepisów prawa.

f) IOD uwzględniając wniosek przekazuje do właściwych jednostek/komórek organizacyjnych Administratora Danych i Podmiotu Przetwarzającego informację o konieczności ograniczenia przetwarzania danych osobowych.

g) Ograniczenie nie dotyczy:

- przechowywania danych,
- celu ustalenia, dochodzenia lub obrony roszczeń,
- ochrony praw innej osoby fizycznej lub prawnej,
- lub gdy zachodzi ważny interes publiczny.

h) Kierownicy jednostek/komórek organizacyjnych odpowiadają IOD w ciągu 14 dni o zastosowaniu się do uzasadnionego wniosku oraz o wszelkich krokach podjętych w celu ograniczenia przetwarzania.

i) IOD sporządza informację dla osoby, której dane dotyczą w terminie 30 dni od dnia wpływu wniosku, uwzględniając, wniosek w części lub całości. Jednocześnie IOD ma prawo scedować obowiązek przygotowania odpowiedzi na merytoryczną jednostkę/komórkę organizacyjną.

j) IOD odnotowuje rejestrze fakt dokonania sprostowania, bądź przesłania informacji o brak dokonania sprostowania, podając datę i formę odpowiedzi wraz z kopią wniosku i udzielonej odpowiedzi.

k) Przed uchyleniem ograniczenia przetwarzania IOD informuje o tym fakcie osobę, której dane dotyczą.

6) Prawo do przenoszenia danych.

a) Na wniosek osoby, której dane dotyczą Nadleśnictwo realizuje prawo do przenoszenia danych.
b) Wniosek winien zawierać co najmniej imię i nazwisko oraz dane identyfikujące wnioskodawcę.
c) Za prawidłowość wypełnienia obowiązku odpowiedzialny jest IOD, który w tym zakresie związany jest postanowieniami wniosku i powszechnie obowiązujących przepisów prawa.
d) IOD przesyła zlecenie właściwych jednostek/komórek organizacyjnych Administratora Danych i Podmiotu Przetwarzającego o przygotowanie danych osobowych, osoby składającej wniosek, przetwarzanych w podległych im zbiorach w formacie nadającym się do odczytu maszynowego.
e) Kierownicy jednostek/komórek organizacyjnych Administratora Danych i Podmiotu Przetwarzającego przygotowują w terminie 14 dni dane osobowe, osoby która złożyła wniosek, w ustrukturyzowanej, powszechnie używanej formie nadającej się do odczytu maszynowego.
f) Przygotowaną informację IOD przekazuje w terminie 30 dni od dnia wpłynięcia wniosku, w przyjętej przez osobę, której dane dotyczą, formie (np. płyta CD, e-mail), stosując przy tym wszelkie niezbędne środki bezpieczeństwa. Jednocześnie IOD ma prawo scedować obowiązek przygotowania odpowiedzi na merytoryczną jednostkę/komórkę organizacyjną.
g) IOD odnotowuje rejestrze fakt udzielenia odpowiedzi na wniosek z podaniem daty i formy udzielonej odpowiedzi wraz z kopia wniosku i udzielonej odpowiedzi.
h) Na żądanie wnioskodawcy jego dane osobowe mogą zostać przesłane bezpośrednio innemu administratorowi danych o ile jest to technicznie możliwe.

7) Prawo do sprzeciwu

a) Mając na względzie prawo osoby, której dane dotyczą, do wniesienie sprzeciwu wobec przetwarzania jej danych przez Nadleśnictwo realizuje się to prawo poprzez zaprzestanie dalszego przetwarzania danych osoby, która wystąpiła z wnioskiem, chyba że zostaną wykazane ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
b) Osoba, która wnosi sprzeciw, winna zwrócić się z wnioskiem zawierającym minimum imię i nazwisko oraz dane ją identyfikujące, a także w przypadku sprzeciwu związanego z jej szczególną sytuacją uzasadnienie zawierające opis przyczyn związanych z jej szczególną sytuacją motywujących wniesienie sprzeciwu. Jeżeli zachodzi konieczność Administrator danych kontaktuje się z Wnioskodawcą w celu ustalenia operacji danych, w ramach których przetwarzanie mogło mieć miejsce.
c) Za prawidłową realizację wniosku odpowiedzialny jest IOD lub dedykowana jednostka we współpracy z IOD. IOD niezwłocznie po otrzymaniu wniosku przekazuje informację o uzasadnionym sprzeciwie właściwym

jednostkom/komórkom organizacyjnych Administratora Danych i Podmiotu Przetwarzającego.

d) Szczególnie umotywowanym wnioskiem podlegającym bezwzględnemu wykonaniu jest sprzeciw wobec przetwarzania na potrzeby marketingu bezpośredniego. W takim przypadku pracownik, który otrzymał od osoby, której dane dotyczą informacje o sprzeciwie wobec działań marketingowych niezwłocznie oznacza sprzeciw w systemie do tego przeznaczonym i informuje o tym fakcie IOD.

e) W sytuacji określonej w ppkt. b) i c) w terminie 14 dni właściwe jednostki/komórki organizacyjne przekazują do IOD informację potwierdzając wykonanie wniosku.

f) W terminie 30 dni od dnia otrzymania wniosku IOD lub dedykowana jednostka informuję osobę go składającą o zrealizowaniu bądź odmowie realizacji wniosku. Odmowa realizacji wniosku musi zostać umotywowana wskazaniem ważnych prawnie uzasadnionych podstaw do dalszego przetwarzania. Jednocześnie IOD ma prawo scedować obowiązek przygotowania odpowiedzi na merytoryczną jednostkę/komórkę organizacyjną.

g) IOD odnotowuje lub rejestrze fakt udzielenia odpowiedzi na wniosek wraz z podaniem daty i sposobu odpowiedzi oraz kopia wniosku i udzielonej odpowiedzi.

8) Prawo do wniesienia odwołania od zautomatyzowanego podejmowania decyzji

a) We wszystkich przypadkach, w których dochodzi do zautomatyzowanego podejmowania decyzji względem osoby, której dane dotyczą, które wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, Nadleśnictwo gwarantuje możliwość odwołania się od decyzji podjętej w taki sposób.

b) Odwołanie, o którym mowa w pkt a) polega na zagwarantowaniu tak zwanej interwencji ludzkiej, w przypadku gdy osoba, której dane dotyczą tego zażąda.

c) Wniosek o interwencję ludzką winien zawierać co najmniej imię i nazwisko oraz inne dane identyfikujące osobę, która go składa, a także zaznaczenie żądania interwencji ludzkiej względem decyzji podjętej w sposób zautomatyzowany.

d) Jeżeli zachodzi konieczność Administrator danych kontaktuje się z Wnioskodawcą w celu ustalenia operacji danych, w ramach których przetwarzanie mogło mieć miejsce.

e) Za prawidłowe wykonanie wniosku odpowiada IOD. IOD przekazuje go do właściwych jednostek/komórek organizacyjnych.

f) Jednostka/komórka organizacyjna po rozpatrzeniu sprawy podejmuje decyzję w zakresie uznania bądź odrzucenia odwołania od zautomatyzowanej decyzji, w terminie do 14 dni.

g) W terminie 30 dni od dnia wpłynięcia wniosku IOD przekazuje osobie, która go złożyła decyzję komórki merytorycznej w sprawie odwołania. Jednocześnie IOD ma prawo scedować obowiązek przygotowania odpowiedzi na merytoryczną jednostkę/komórkę organizacyjną.

h) IOD odnotowuje w rejestrze fakt udzielenia odpowiedzi na wniosek wraz z odnotowaniem daty i formy odpowiedzi oraz kopii wniosku i udzielonej odpowiedzi.

9) Postanowienia wspólne.

a) We wszystkich przypadkach, w których niezbędne jest współpraca a administratorem SILP dla prawidłowości wykonania wniosku, administrator SILP zobowiązany są do pełnego współdziałania z pozostałymi komórkami merytorycznymi i w tym zakresie wpierają IOD.

b) We wszystkich przypadkach, w których jest to możliwe, w celu prawidłowego wykonania wniosku osoby, której dane dotyczą, dopuszczalne jest wykorzystanie wewnętrznych i zewnętrznych systemów informatycznych, system zgłoszeniowy itp.

c) Każdemu pracownikowi przysługują wszystkie powyższe prawa osób, których dane dotyczą. Równocześnie pracownik ma prawo w celach administracyjno kadrowych zwrócić się bezpośrednio do komórki kadrowej.

d) Przed realizacja każdego wniosku dotyczącego prawa do usuniecie danych (bycia zapomnianym, przenoszenia danych, dostępu do danych i ograniczenia przetwarzania), w związku z dużym ryzykiem naruszenia praw i wolności osoby, której wniosek dotyczy, należy obligatoryjnie zweryfikować tożsamość Wnioskodawcy poprzez:

- okazanie dowodu tożsamości
- przesłanie korespondencji elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym
- pisemnym wnioskiem.

e) O możliwości wykorzystania danego systemu oraz sposobie jego dostosowania do realizacji niniejszej procedury decyduje IOD.

f) W celu zachowania rozliczalności wszelkie czynności podejmowane na podstawie niniejszej procedury winny zostać udokumentowane.

g) Całość dokumentacji związanej z wykonaniem wniosku gromadzi i przechowuje IOD lub dedykowana jednostka.

Załącznik 6.

Aktualizacja / Nowe upoważnienie *

Upoważnienie nr _____

Pan/Pani …… , zatrudniona/zatrudniony odbywająca/odbywający staż w Nadleśnictwie do przetwarzania danych osobowych (w systemie informatycznym oraz w formie papierowej) w czasie trwania stosunku pracy.

Upoważniona/upoważniony zobowiązany jest do:

1. Ochrony danych osobowych w systemie informatycznym i przetwarzanych w postaci papierowej, a w szczególności przeciwdziałaniu dostępowi osób niepowołanych.
2. Przestrzegania zasad określonych w Polityce Ochrony Danych.
3. Przestrzegania zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.
4. Zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.

Niniejszym upoważniam Panią / Pana _____ do przetwarzania danych osobowych w Nadleśnictwie Ciechanów w zakresie wypełnienia zadań wynikających z obowiązków służbowych na stanowisku …… / obowiązków wynikających z realizacji umowy ... (numer umowy)*.

Nadaję upoważnienie

.....

(data, podpis, pieczątka Administratora Danych)

* niewłaściwe skreślić

……

Miejscowość , data

.....
(imię i nazwisko)

.....
(stanowisko służbowe)

.....
(nazwa komórki organizacyjnej)

OŚWIADCZENIE

Oświadczam, że zostałam (łem) poinformowana (y) o ciążącym na mnie obowiązku przetwarzania i ochrony danych osobowych zgodnie z wymogami wynikającym i z wewnętrznych regulacji z zakresu ochrony danych osobowych obowiązujących w Nadleśnictwie Ciechanów w tym w szczególności w Polityce Ochrony Danych, jak również zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

W szczególności zobowiązana (y) jestem – w stopniu wynikającym z realizacji zadań wynikających z umowy o pracę/umowy cywilno-prawnej – do przeciwdziałania dostępowi osób nieuprawnionych do systemów informatycznych, kartotek, skorowidzów, ksiąg, wykazów i inny zbiorów ewidencyjnych, w których są przetwarzane dane osobowe.

Ponadto zobowiązuję się do natychmiastowego powiadomienia swoich przełożonych o każdym zauważonym przeze mnie przypadku naruszenia stosowanych w Nadleśnictwie zasad bezpieczeństwa wobec danych osobowych.

Zobowiązuję się do zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

……

czytelny podpis Oświadczającego

Załącznik nr 7.

Numer upoważnienia	Imię i nazwisko osoby upoważnionej	Login w systemie informatycznym	Stanowisko/Numer umowy	Data nadania upoważnienia	Data odebrania upoważnienia

Załącznik nr 8.

Załącznik 8.

L.p.	Naruszenie	Data i godzina zgłoszenia podejrzenia naruszenia	Data oraz godzina stwierdzenia naruszenia	Data naruszenia/okres, którego dotyczy	Kategoria i ilość osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Osoba/źródło informacji o zdarzeniu	Miejsce naruszenia	Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia	Opis skutków/konsekwencji naruszenia	Osoba/jednostka odpowiedzialna za naruszenie	Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym zastosowane środki zastosowane w celu zminimalizowania jego negatywnych skutków	Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (Jeśli tak - data i godzina zgłoszenia; w przypadku wystąpienia opóźnienia w powiadomieniu - wyjaśnienie przyczyn opóźnienia)	Czy poinformowano organy ścigania (data zawiadomienia)	Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy oraz sposób przekazania informacji wraz opisem zaleceń dla podmiotów danych	Monitoring działań naprawczych
1																	
2																	
3																	
4																	

Załącznik nr 9.

Instrukcja zarządzania systemem informatycznym

w NADLEŚNICTWIE CIECHANÓW

Spis treści

Rozdział 1.Postanowienia ogólne.

§ 1.

Definicje.

Termin	Znaczenie
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnie rozporządzenie o ochronie danych)
Klauzula zgoda podmiotu danych	Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych
Klauzula informacyjna	Informowanie osób, których dane dotyczą, o wykorzystywaniu ich danych osobowych (prowadzeniu operacji przetwarzania) i celach, dla których jest ono prowadzone oraz jest niezbędne dla zapewnienia rzetelności i przejrzystości przetwarzania danych osobowych.
Administrator danych	Nadleśnictwo Ciechanów, która ustala cele i sposoby przetwarzania danych osobowych.
Podmiot przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych.
Inspektor Ochrony Danych (IOD)	Osoba fizyczna powołana zarządzeniem Nadleśniczego do wspierania Administratora Danych w przestrzeganiu postanowień RODO.
Administrator Systemów Informatycznych (ASI) –	osoba fizyczna wyznaczona przez Administratora Danych Osobowych, zajmująca się sprawowaniem ogólnego nadzoru nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym danych osobowych przetwarzanych w systemie informatycznym;
Kierownik jednostki/ komórki organizacyjnej	Nadleśniczy/Kierownik lub samodzielne stanowisko bezpośrednio podległe pod Nadleśniczego.
Dane osobowe	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, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
Zbiór danych osobowych	Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
Przetwarzanie danych osobowych	Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Termin	Znaczenie
Naruszenie ochrony danych osobowych	Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
Profilowanie	Dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było 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,
Ograniczenie przetwarzania danych osobowych	Oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
Specjalne kategorie danych	Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
Pracownik	Osoba fizyczna zatrudniona w Nadleśnictwie na podstawie umowy o pracę lub powołania.
Współpracownik	Osoba fizyczna współpracująca ze Nadleśnictwem w oparciu o umowę zlecenia, o dzieło i inne umowy o charakterze cywilnoprawnym, jak też praktykant, stażysta, wolontariusz, pracownik tymczasowy - wykonujący pracę lub realizujący czynności zlecone na rzecz Nadleśnictwa.
System teleinformatyczny	Wydzielony zespół współpracujących ze sobą urządzeń oraz oprogramowania, przetwarzający dane osobowe w postaci elektronicznej.
zabezpieczenie danych w systemie informatycznym	wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
Baza danych osobowych	zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe
Hasło	ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym
Identyfikator / login	ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych

Termin	Znaczenie
	osobowych w systemie informatycznym
IZSI / Instrukcja	niniejszy dokument
AD	Active Directory usługa katalogowa, katalog użytkowników i komputerów pracujących w sieci LP, zdefiniowana osobnym dokumentem „Projekt usług katalogowych PGL LP”
Kopia pełna	kopia zapasowa całości danych osobowych przetwarzanych w systemie informatycznym
Elektroniczne nośniki danych	przedmioty fizyczne, na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych
System informatyczny (system IT)	zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych
SILP	Zintegrowany System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu zasobów informatycznych LP.
Sieć publiczna	sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych
Teletransmisja	przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
Uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu
Użytkownik	wyznaczony do przetwarzania danych osobowych pracownik, który odbył stosowne szkolenie w zakresie ochrony tych danych oraz uzyskał upoważnienie i uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

§ 2.

Cel i zakres stosowania instrukcji.

1. Podstawowym celem zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych jest zapewnienie jak najwyższego standardu bezpieczeństwa tych danych. Priorytetowe jest zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemów informatycznych stosowanych w Nadleśnictwie Ciechanów;
2. Istotnym elementem osiągnięcia celu, o którym mowa w ust. 1 jest zapewnienie odpowiedniego poziomu oraz kontroli dostępu:
    1) do sieci, w tym urządzeń serwerowych,
    2) do systemów operacyjnych,

3) do aplikacji,
4) do informacji i zbiorów danych, wraz z określeniem trybu dostępu.

3. **Szczegółowe zasady zarządzania systemem informatycznym Nadleśnictwa Ciechanów reguluje Załącznik nr 2 do Zarządzenia Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017r znak sprawy OI.0413.13.2017 – „Zasady Bezpiecznej Eksploatacji Zasobów Informatycznych Lasów Państwowych"**

§ 3.

Konfiguracja sprzętu komputerowego użytkownika systemu.

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych oraz logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym kontroli przepływu informacji pomiędzy system a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu;
1. Każdy dostęp do danych osobowych jest zarejestrowany;
2. Urządzenie mobilne (laptop, tablet itp.) zawierające dane osobowe jest zabezpieczone przed nieuprawnionym dostępem;
3. Minimalne środki ochrony to:
   1) zainstalowanie na stacjach zapory sieciowej firewall i oprogramowania antywirusowego,
   2) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników,
   3) wymaganie podania hasła przed uzyskaniem dostępu do systemu operacyjnego,
   4) niepozostawianie niezablokowanych stacji roboczej bez nadzoru,
   5) praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

§ 4.

1. Użytkownik jest zobowiązany do stałego monitorowania komunikatów pochodzących z oprogramowania antywirusowego zainstalowanego na stacji roboczej oraz na urządzeniach mobilnych i reagowania na nie;
2. W przypadku niesprawdzenia przez Użytkownika systemu pliku dostarczonego z zewnątrz, oprogramowanie antywirusowe automatycznie chroni system poprzez monitorowanie plików w stanie rzeczywistym. W przypadku wykrycia zagrożenia, oprogramowanie stosownie reaguje na to zagrożenie.

Rozdział 2.Procedury nadawania uprawnień. Metody i środki uwierzytelniania.

§ 5.

Procedury nadawania, modyfikacji, zabierania uprawnień.

1. Nowemu pracownikowi – Użytkownikowi SILP, ASI przydziela login i tymczasowe hasło; dodaje pracownika do domeny LP, wysyła do RDLP w Olsztynie formularz z danymi pozwalającymi założenie poczty elektronicznej w domenie „lasy.gov.pl",
2. Administrator udziela instruktażu związanego z wykorzystaniem systemów komputerowych w Nadleśnictwie z uwzględnieniem zasad bezpieczeństwa oraz ochrony antywirusowej.
3. Pracownik zobowiązany jest do zapoznania się z Zarządzeniem nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w PGL-LP,
4. Pracownik, w zakresie powierzonych mu obowiązków zobowiązany jest do zapoznania się z „**Polityka ochrony danych osobowych**" Nadleśnictwa Ciechanów
5. Po otrzymaniu hasła tymczasowego Użytkownik ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz jego zmiany na hasło osobiste;

6. Zakazuje się przekazywania haseł tymczasowych poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np. przez niechronione wiadomości przekazywane elektronicznie;
7. ASI dokonuje rejestracji i prowadzi wykaz loginów przydzielonych poszczególnym Użytkownikom, który wiąże loginy z imiennie wskazanymi pracownikami;
8. Dostęp do systemu informatycznego służącego do przetwarzana danych osobowych może uzyskać wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez ADO;
9. Uprawnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych nadaje ASI na wniosek osoby odpowiedzialnej za daną komórkę organizacyjną Nadleśnictwa po zatwierdzeniu przez Nadleśniczego;
10. Uprawnienia, o których mowa w ust. 7 określają poziom dostępu do sieci, w tym urządzeń serwerowych, do systemów operacyjnych, do aplikacji i informacji;
11. Użytkownikom nadawane są uprawnienia do prac tylko w modułach i funkcjach programu wymaganych dla realizacji powierzonych im zadań*;*
12. Użytkownik systemu informatycznego ponosi odpowiedzialność za bezpieczeństwo danych osobowych przetwarzanych we wszystkich operacjach wykonanych przy użyciu jego loginu i hasła dostępu;
13. W przypadku wygaśnięcia przesłanek uprawniających Użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia do ich przetwarzania lub wygaśnięcia stosunku pracy, ASI przy współpracy z IOD zobowiązany jest do wyrejestrowania Użytkownika z systemu informatycznego, do którego był uprawniony. W takiej sytuacji Użytkownik zobowiązany jest do przekazania sprzętu informatycznego, wszelkich posiadanych cyfrowych nośników informacji w szczególności zawierających kopie dokumentów oraz posiadanej karty kryptograficznej.
14. Wyrejestrowanie Użytkownika z ewidencji osób upoważnionych do przetwarzania informacji następuje poprzez zablokowanie go we wszystkich opcjach systemu informatycznego, do których miał dostęp.

§ 6.

Metody oraz środki uwierzytelniania,

1. Podstawowym systemem uwierzytelniania użytkowników i administratorów na stacjach roboczych systemu informatycznego jest uwierzytelnienie kartą kryptograficzną i certyfikatem korporacyjnym PKI LP.
2. Dopuszcza się uwierzytelnianie w oparciu o system usług katalogowych AD – tj z wykorzystaniem indywidualnej nazwy((identyfikatora/loginu) i hasła użytkownika.;
3. Celem stosowania identyfikatora (loginu) Użytkownika jest jednoznaczne określenie osoby, która się nim posługuje;
4. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika, ASI za zgodą IOD nadaje inny identyfikator, odstępując od zasady określonej w ust. 2;
5. System informatyczny, w którym przetwarzane są dane osobowe automatycznie wymusza podanie identyfikatora i hasła Użytkownika;

§ 7.

1. Hasło Użytkownika:
    1) musi się składać co najmniej z 8 znaków, (zalecane 10 znaków) w tym zawierać małe i wielkie litery oraz cyfry lub znaki specjalne**,**
    2) nie może zawierać znaków następujących po sobie na klawiaturze bądź tych samych liter lub cyfr,
    3) nie może zawierać imion, nazwisk, pseudonimów, inicjałów, dat, numerów rejestracyjnych samochodów, numerów telefonów i innych kombinacji znaków mogących doprowadzić do łatwego rozszyfrowania go przez osoby nieupoważnione,

4) nie może zawierać identyfikatorów (loginów),
5) nie może być zapisywane w systemie w postaci jawnej**,**
6) nie może być wyświetlane na ekranie komputera w sposób jawny**,**
7) nie może być ujawnione innej osobie, nawet po utracie ważności**,**
8) musi być zabezpieczone przez Użytkownika przed nieuprawnionym dostępem osób trzecich;

2. W przypadku nieumyślnego ujawnienia hasła osobie nieuprawnionej lub podejrzenia ujawnienia, należy bezzwłocznie powiadomić ASI i dokonać zmiany hasła na nowe**;**
3. System informatyczny, w którym przetwarzane są dane osobowe automatycznie wymusza zmianę hasła **nie rzadziej niż co 90 dni**;
4. ASI może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez Użytkownika oraz zapewniać automatyczną weryfikację spełniania wymogów dotyczących hasła**;**

§ 8.

Wygaszacze ekranu.

1. Wygaszacze ekranu systemowo ustawiane są na aktywację po 10 minutach bezczynności na danej stacji roboczej oraz w razie potrzeby (np. opuszczenie miejsca przetwarzania danych) skrótem klawiaturowym;
2. Uruchomienie wygaszacza ekranu wiąże się z koniecznością ponownego zalogowania, celem wznowienia pracy stacji roboczej.

Rozdział 3.Procedury rozpoczynania, zawieszania i kończenia pracy w systemie informatycznym.

§ 9.

Rozpoczęcie pracy.

1. Procedura rozpoczęcia pracy w systemie informatycznym następuje poprzez zalogowanie się Użytkownika do komputera przez podanie loginu i hasła dostępu;
2. W przypadku 5-krotnego wprowadzenia błędnych danych (login, hasło), dostęp zostanie zablokowany, o czym należy niezwłocznie zawiadomić ASI;
3. W przypadku zapomnienia przez Użytkownika konstrukcji hasła, winien on niezwłocznie zawiadomić ASI, który nadaje nowe hasło, postępując zgodnie z procedurą obowiązującą przy nadawaniu uprawnień dostępu do systemu informatycznego.

§ 10.

Zawieszenie pracy.

1. Ustala się następującą procedurę zawieszenia pracy w systemie informatycznym:
   1) przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby osoby postronne nie miały dostępu do danych przetwarzanych na tym stanowisku,
   2) każdy Użytkownik ma obowiązek stosowania wygaszacza ekranu zabezpieczonego hasłem oraz wylogowania się z systemu lub jego blokowania,
   3) zablokowanie komputera odbywa się poprzez naciśnięcie kombinacji klawiszy,
   4) niezależnie od powyższego, wygaszacz ekranu aktywuje się nie później niż w 10 minucie bezczynności Użytkownika,
   5) odblokowanie odbywa się poprzez ponowne zalogowanie się tego samego Użytkownika,
2. W pomieszczeniu, w którym przetwarzane są dane osobowe mogą znajdować się osoby postronne wyłącznie za zgodą i w towarzystwie Użytkownika lub innej upoważnionej osoby;
3. W przypadku zawieszenia pracy w systemie informatycznym z powodu konieczności załatwienia sprawy z osobą postronną znajdującą się w tym samym pomieszczeniu, Użytkownik ma obowiązek zabezpieczenia ekranu komputera lub urządzenia mobilnego oraz dokumentów i wydruków znajdujących się na biurku w sposób uniemożliwiający podgląd zawartych w nich treści.

§ 11.

Zakończenie pracy.

1. Zakończenie pracy w systemie informatycznym polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy;
2. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien pozostać przy komputerze do chwili ich zamknięcia;
3. Użytkownik kończący pracę powinien sprawdzić, czy wszystkie elektroniczne nośniki informacji lub wydruki i dokumenty zawierające dane osobowe zostały zabezpieczone przed dostępem osób nieupoważnionych;
4. Osoba opuszająca pomieszczenie jako ostatnia powinna zamknąć okna oraz zamknąć drzwi od pomieszczenia na klucz.

Rozdział 4 Procedury użytkowania urządzeń mobilnych i elektronicznych nośników informacji. Korzystanie z Internetu. Poczta elektroniczna.

§ 12.

1. Przy przetwarzaniu danych osobowych na urządzeniach mobilnych oraz elektronicznych nośnikach informacji należy stosować procedury obowiązujące w przypadku użytkowania komputerów i urządzeń stacjonarnych;
2. Użytkownicy, którym zostały powierzone urządzenia mobilne oraz elektroniczne nośniki informacji, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Szczególną ostrożność należy zachować podczas ich transportu;
3. Obowiązuje zakaz używania urządzeń mobilnych oraz elektronicznych nośników informacji przez osoby inne niż Użytkownicy, którym zostały one powierzone;
4. Pliki zawierające dane osobowe przechowywane na urządzeniach mobilnych, elektronicznych nośnikach informacji muszą być zaszyfrowane i opatrzone hasłem dostępu;
5. Urządzenia mobilne i elektroniczne nośniki informacji muszą być wyposażone w odpowiednie programy ochrony antywirusowej. Za tryb i sposób aktualizowania programów ochrony antywirusowej na urządzeniach mobilnych i elektronicznych nośników informacji odpowiada ASI.

§ 13.

Korzystanie z Internetu.

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych;
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach;
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu bez zgody i wiedzy ASI;
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo;
5. W opcjach przeglądarki internetowej zabrania się włączania opcji autouzupełniania formularzy i zapamiętywania haseł;
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właściciel certyfikatu jest wiarygodny;

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podawania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

§ 14.

Poczta elektroniczna.

1. System poczty elektronicznej LP obsługuje skrzynki poczty elektronicznej w domenach i subdomenach będących własnością Lasów Państwowych.
2. Użytkownicy kont pocztowych zawartych w domenie LP muszą przestrzegać „Regulaminu użytkowania systemu poczty elektronicznej LP". Aktualny „Regulamin użytkowania systemu poczty elektronicznej LP" publikowany jest pod adresem http://poczta.lasy.gov.pl/regulamin .
3. Przesyłanie danych osobowych z użyciem poczty elektronicznej może odbywać się tylko przez osoby do tego upoważnione;
4. W przypadku przesyłania danych osobowych należy wykorzystywać mechanizmy kryptograficzne;
5. Hasło zabezpieczające wysyłane pliki powinno zawierać minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne. Hasło należy przesłać adresatowi inną metodą, np. telefonicznie lub SMS-em;
6. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu wysyłanego pocztą elektroniczną;
7. Zaleca się, aby Użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata;
8. Bez weryfikacji wiarygodności nadawcy zabrania się otwierania nieznanych załączników (plików) otrzymanych w e-mailach nawet od znanych nadawców;
9. Bez weryfikacji wiarygodności nadawcy, zabrania się „klikać" na hiperlink w otrzymanym e-mailu;
10. Każdy przypadek otrzymania e-maila o wątpliwej wiarygodności należy zgłaszać do ASI;
11. Zabrania się rozsyłania wiadomości prywatnych z wykorzystaniem konta służbowego;
12. Przy wysyłaniu korespondencji zbiorowej należy zawsze użyć opcji UDW – ukryte do wiadomości;
13. Użytkownicy mają prawo korzystać ze służbowej poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie w sposób ograniczony do niezbędnego minimum;
14. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych;
15. Przy korzystaniu z poczty elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego;
16. Użytkownicy nie mogą korzystać ze służbowej poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania (molestowanie, mobbing)
17. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

Rozdział 5 Zabezpieczanie danych w systemie informatycznym.

§ 15.

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

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

2. Za tworzenie i przechowywanie kopii zapasowych, o których mowa w ust. 1, niniejszej Instrukcji odpowiedzialny jest ASI;
3. Dostęp do kopii zapasowych posiada wyłącznie ASI lub w wyjątkowych wypadkach, osoba upoważniona przez ADO.

§ 16.

Sposób, miejsce i okres przechowywania kopii zapasowych i elektronicznych nośników informacji

1. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
2. Kopie zapasowe i elektroniczne nośniki informacji przechowywane są przez okres, w którym istnieją przesłanki do ich przetwarzania. Po ustaniu przesłanek, o których mowa w zdaniu pierwszym, dane znajdujące się na kopiach zapasowych muszą zostać usunięte w sposób uniemożliwiający ich odtworzenie;
3. Kopie awaryjne należy bezzwłocznie usuwać po ustaniu ich użyteczności w przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych.

§ 17.

Sposób zabezpieczania systemu informatycznego.

1. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji, stanowiących tajemnicę służbową przed ich nieuprawnionym przetwarzaniem oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej;
2. System informatyczny musi być chroniony równolegle na wielu poziomach m.in. poprzez stosowanie oprogramowania antywirusowego, systemów typu firewall, aktualizacje systemu operacyjnego oraz realizację kopii bezpieczeństwa;
3. Oprogramowanie antywirusowe jest instalowane na wszystkich stanowiskach komputerowych oraz urządzeniach mobilnych i elektronicznych nośnikach informacji;
4. Aktualizacja oprogramowania antywirusowego odbywa się nie rzadziej niż raz w tygodniu, w sposób automatyczny dla wszystkich komputerów zainstalowanych w sieci;
5. Użytkownik na stanowisku komputerowym, importujący dane do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów i szkodliwego oprogramowania;
6. O pojawiających się komunikatach wskazujących na wystąpienie zagrożenia spowodowanego szkodliwym oprogramowaniem, Użytkownik jest zobowiązany niezwłocznie powiadomić ASI;
7. Za wdrożenie, oraz aktualizację i korzystanie z oprogramowania, o którym mowa w ust. 2 odpowiada ASI.

§ 18.

Monitorowanie systemu informatycznego.

1. W celu zapewnienia ochrony systemu informatycznego stosuje się monitoring wykorzystania infrastruktury informatycznej, w szczególności obejmujący następujące elementy:
    1) analizę oprogramowania wykorzystanego na stacjach roboczych;
    2) analizę stacji roboczych pod względem wykorzystania nielegalnego oprogramowania, plików multimedialnych oraz innych elementów naruszających prawo autorskie;
    3) analizę odwiedzanych stron www;
    4) analizę godzin pracy na stanowiskach komputerowych;
    5) analizę dostępów (autoryzowanych oraz nieautoryzowanych);
    6) analizę ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych przetwarzanych w systemie;

2. Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.

§ 19.

Obowiązki ASI w zakresie zabezpieczenia systemu informatycznego

1. Do obowiązków ASI w zakresie zabezpieczenia systemu informatycznego należy :
    1) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemów,
    2) nadzór nad czynnościami związanymi ze sprawdzaniem systemów pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji,
    3) nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych,
    4) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
    5) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych, w tym zarządzanie kontami użytkowników (ustalenie identyfikatorów i haseł, ich przyznawanie, anulowanie, resetowanie i ochrona) oraz w porozumieniu z IOD dbałość o właściwe ustawienie urządzeń, tak aby minimalizować możliwość nieuprawnionego dostępu,
    6) podejmowanie natychmiastowych działań zabezpieczających stan systemów informatycznych w przypadku otrzymania informacji o naruszeniu zabezpieczeń, informacji o zmianach w sposobie działania systemu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych, w tym podjęcie działań mających na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie.

§ 20.

1. W celu zabezpieczenia integralności systemu informatycznego ASI może wykorzystywać w trakcie pracy oprogramowanie lub narzędzia monitorujące i rejestrujące aktywność Użytkowników na stanowiskach komputerowych;
2. Zabezpieczenie integralności systemu informatycznego realizowane jest również poprzez zakaz:
    1) wysyłania masowej poczty kierowanej do losowych odbiorców (spam),
    2) przechowywania w systemie informatycznym treści łamiących prawo autorskie (filmy, utwory muzyczne lub oprogramowanie),
    3) nieuzasadnionego wynoszenia lub wysyłania danych osobowych poza obszar przetwarzania danych,
    4) instalowania przez Użytkownika oprogramowania na sprzęcie komputerowym, które nie uzyskało akceptacji ASI,
    5) wykorzystywania przeglądarek internetowych, które nie uzyskały akceptacji ASI oraz odwiedzania witryn internetowych zawierających potencjalnie niebezpieczne treści,
    6) podłączania innych urządzeń niż teleinformatyczne do wydzielonej instalacji elektrycznej (gniazdka w kolorze czerwonym),
    7) przemieszczania sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany Użytkownika bez uzgodnienia z ASI;
    8) fizycznego ingerowania w konfigurację sprzętową urządzeń,
    9) podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchanie lub przechwycenie informacji przepływających w systemach informatycznych,

3. Dla zachowania integralności systemu informatycznego ASI może podjąć decyzję o:
    1) deinstalacji niebezpiecznego oprogramowania,
    2) usunięciu nielegalnych, niebezpiecznych oraz utrudniających wykonanie kopii bezpieczeństwa plików,
    3) zablokowaniu dostępu Użytkownika w przypadku stwierdzenia, że komputer lub urządzenie dołączone generuje strumień danych zakłócający pracę sieci lub w razie podejrzenia używania komputera jako niezarejestrowanego serwera danych. O tym fakcie powiadamiany jest IOD i bezpośredni przełożony Użytkownika,
    4) w porozumieniu z IOD, zablokowaniu konta Użytkownika.

§ 21.

Procedury wykonywania przeglądów i konserwacji systemu informatycznego.

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację platformy sprzętowej, na której eksploatowany jest system informatyczny wykorzystywany w Nadleśnictwie;
2. Przeglądy i konserwacja urządzeń wchodzących w skład platformy sprzętowej, o której mowa w ust. 1 powinny być wykonywane nie rzadziej niż w terminach określonych przez producenta sprzętu;
3. Jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych lub nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ASI;
4. Wszelkie naprawy urządzeń komputerowych, w tym urządzeń mobilnych i elektronicznych nośników informacji, oraz zmiany w systemie informatycznym przeprowadza, w miarę możliwości, ASI;
5. Jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI;
6. W przypadku niemożności dokonania naprawy uszkodzonego sprzętu komputerowego zawierającego dane osobowe, należy go zniszczyć mechanicznie w sposób trwale uniemożliwiający odczytanie jego zawartości;
7. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez Użytkownika potrzeby wprowadzenia zmian pozwalających dostosować ich funkcjonalność do obsługi bieżących lub planowanych potrzeb. Zgłoszenia rozpatruje ASI;
8. Nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane przez ASI;
9. Przegląd aplikacji przeprowadzany jest w celu sprawdzenia poprawności działania i wykonywany jest w następujących przypadkach:
    1) zmiany wersji oprogramowania aplikacji,
    2) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowana jest aplikacja,
    3) wykonania zmian w aplikacji spowodowanych koniecznością naprawy lub modyfikacji systemu;
10. Przed dokonaniem zmian w aplikacji należy, o ile to możliwe, dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych, na testowej bazie danych. Sprawdzenie powinno obejmować w szczególności:
    1) poprawność logowania się do systemu w zależności od posiadanych uprawnień (symulacja pracy wszystkich typów uprawnień Użytkownika),
    2) techniczną poprawność działania aplikacji.

Procedura niszczenia danych na nośnikach elektronicznych.

§ 22.

1. W odniesieniu do nośników przenośnych (pen-drive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – utylizowanych lub przeznaczonych do sprzedaży stosowane są mechanizmy bezpiecznego kasowania informacji:
   1) za pomocą specjalistycznego oprogramowania,
   2) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników;
2. Nośniki elektroniczne, które mogą być ponownie wykorzystane lub przeznaczone są do sprzedaży (przekazania) czyszczone są przez ASI z wykorzystaniem specjalistycznego oprogramowania. Czynność ta jest dokumentowana stosownym protokołem generowanym przez program.
3. Nośniki elektroniczne, które nie mogą być ponownie wykorzystane, są niszczone mechanicznie lub oddawane do utylizacji przez firmę specjalistyczną;
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada ASI
5. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia, sporządzonym przez komisję likwidacyjną Nadleśnictwa w obecności ASI.

Rozdział 6 Postanowienia końcowe.

§ 23.

1. Nad aktualnością Instrukcji czuwa IOD w porozumieniu z ASI;
2. IOD we współpracy z ASI może prowadzić kontrolę przestrzegania Instrukcji. Wyniki kontroli doraźnych przedstawiane są ADO.