Załącznik nr 1 do Zarządzenia nr 11 Nadleśniczego
Nadleśnictwa Opole z dnia 1.02.2021 r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służąca do przetwarzania danych osobowych w Nadleśnictwie Opole

ROZDZIAŁ I

Zasady ogólne

§ 1

Wprowadza się Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącą do przetwarzania danych osobowych w Nadleśnictwie Opole.

§ 2

Zobowiązuje się pracowników Nadleśnictwa Opole do stosowania zasad określonych w dokumentacji ochrony danych osobowych.

§ 3

1.Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Nadleśnictwie Opole.

2.W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie zasady postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

ROZDZIAŁ II

Podstawowe definicje

§ 1

- Administrator (ADO) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państw członkowskich, to również w prawie Unii lub w prawie państw członkowskich

może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

- Administrator Systemu Informatycznego (ASI) – osoba lub osoby odpowiedzialna/e za prawidłowe funkcjonowanie systemu informatycznego. ASI jest powoływany i odwoływana przez Administratora.
- Inspektor Ochrony Danych (IOD) –osoba powołana przez Administratora w celu zapewnienia stosowania przepisów rozporządzenia oraz dbania o zasady zapisane w niniejszym dokumencie.
- Organ Nadzorczy – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 rozporządzenia.
- Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, 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.
- Przetwarzanie – oznacza operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.
- Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystywaniu 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.
- Zbiór danych – oznacza uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
- Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
- Odbiorca danych - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie

od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mających zastosowanie stosownie do celów przetwarzania.

- Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych. Za naruszenie bezpieczeństwa informacji uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, szafki, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj, na papierze (wydruki), kliszy, folii, zdjęciach, dyskietkach, pamięciach flash itp.w formie niezabezpieczonej.
- Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
- Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
- Sieć publiczna - publiczna sieć telekomunikacyjna w rozumieniu art.2 pkt.29 ustawy z dnia 16 lipca 2004r. Prawo telekomunikacyjne.
- System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- Teletransmisja - przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
- Użytkownik – osoba zatrudniona na umowę o pracę, umowę cywilno-prawną, stażysta lub praktykant w Nadleśnictwie Opole mająca dostęp do komputera z danymi osobowymi w tym przetwarzająca dane osobowe.
- Nadleśnictwo – PGL LP Nadleśnictwo Opole z siedzibą w Opolu przy ul. Groszowickiej 10, 45-517 Opole
- Rozporządzenie - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

ROZDZIAŁ III
Polityka Bezpieczeństwa

Polityka bezpieczeństwa rozumiana jest, jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz nadleśnictwa. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

§ 1
Deklaracja

1.Administrator mając wiedzę, iż przetwarza różne dane osobowe w tym pracowników, petentów, osób które współpracują z nadleśnictwem, deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
2.W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator wprowadza określone niniejszym dokumentem zasady przetwarzania danych. Przedmiotowe zasady określa w szczególności Polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3.Uwzględniając fakt, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy użytkownik upoważniony do przetwarzania danych, pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.
4.W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, w szczególności przez osoby dopuszczone do przetwarzania danych.

§ 2
Charakterystyka Administratora

1. Administratorem jest Państwowe Gospodarstwo Leśne Lasy Państwowe Nadleśnictwo Opole z siedzibą w Opolu przy ul. Groszowickiej 10, 45-517 Opole, reprezentowane przez Nadleśniczego Nadleśnictwa Opole, Pana Marka Cholewę.
2. Administrator realizuje zadania określone w ustawie z dnia 29 września 1991 r. o lasach oraz Statucie Państwowego Gospodarstwa Leśnego Lasy Państwowe stanowiącego załącznik do Zarządzenia nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. uprawniających nadleśnictwo do podejmowania stosownych działań, w tym do przetwarzania danych osobowych. Podstawowym obszarem działania jest szeroko rozumiana gospodarka leśna oraz realizacja w tym zakresie określonych przepisów prawa.

§ 3
Inspektor Ochrony Danych (IOD)

1. Obowiązki Inspektora Ochrony Danych pełni osoba wyznaczona w trybie art. 37 rozporządzenia przez Administratora.
2. IOD powołuje i odwołuje Administrator.
3. Status IOD:
a/. Administrator zapewnia, aby IOD właściwie i niezwłocznie był włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
b/. Administrator zapewnia IOD zasoby niezbędne do wykonywania zadań oraz dostęp do danych osobowych i operacji przetwarzania,
c/. IOD w zakresie wykonywanych zadań podlega bezpośrednio Administratorowi.
4. IOD realizuje zadania w zakresie ochrony danych osobowych, w tym w szczególności;
a/. informuje Administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów o ochronie danych osobowych i doradza im w tej sprawie,
b/. monitoruje przestrzeganie rozporządzenia, innych przepisów o ochronie danych oraz polityki Administratora w dziedzinie danych osobowych, w tym podział obowiązków, działania zwiększające świadomość,
c/. udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonywanie zgodnie z art. 35 rozporządzenia,
d/. współpracuje z Organem Nadzorczym,
e/. pełni funkcje punktu kontaktowego dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia oraz w stosowych przypadkach prowadzi konsultacje we wszystkich innych sprawach.

§ 4

Obowiązek informacyjny

1. W przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą obowiązkiem Administratora jest podczas pozyskiwania danych osobowych przekazanie jej następujących informacji;
a/. swoją tożsamość oraz dane kontaktowe,
b/. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania danych osobowych,
c/. jeżeli przetwarzanie odbywa się na podstawie art.6 lit.f/. – prawnie uzasadnione interesy realizowane przez Administratora lub przez osobę trzecią (np. obrona, ustalanie lub dochodzenie roszczeń, bezpieczeństwo osób i mienia),
d/. informację o odbiorcach danych osobowych lub o kategoriach odbiorców ,
e/. gdy ma to zastosowanie – informację o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
f/. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
g/. informację o prawie żądania od Administratora dostępu do danych osobowych,

ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
h/. jeżeli przetwarzanie odbywa się na podstawie art.6 ust.1 lit.a/. lub art.9 ust.2 lit.a/. – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
i/. informacje o prawie wniesienia skargi do Organu Nadzorczego,
j/. informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje nie podania danych,
k/. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
2. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator podaje osobie dodatkowe informacje o źródle pochodzenia danych osobowych, a gdy to ma zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.
3. Wzór klauzuli w przypadku danych pozyskanych bezpośrednio od osoby, której dane dotyczą stanowi **załącznik nr 1.**
4. Wzór klauzuli w przypadku danych pozyskanych z innych źródeł stanowi **załącznik nr 2.**

§ 5

Dostęp do informacji o osobie, której dane dotyczą

Osoba, której dane dotyczą jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące.
1. Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

- celu przetwarzania,
- kategorii danych osobowych,
- informacji o odbiorcach lub kategorii odbiorców, których dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- informacji o prawie żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
- informacji o prawie wniesienia skargi do Organu Nadzorczego,
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o tym źródle,
- informacji o braku zautomatyzowanego podejmowania decyzji, w tym o braku profilowania,
- jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać

poinformowana o odpowiednich zabezpieczeniach danych związanych z przetwarzaniem.

2. Nadleśnictwo udostępnia osobie, której dane dotyczą, na jej żądanie, kopie danych osobowych podlegających przetwarzaniu.

3. Administrator prowadzi ewidencję realizacji prawa wobec osób, których dane dotyczą według wzoru stanowiącego **załącznik nr 3.**

4. Wzory uprawnień przysługujących osobom stanowią **załączniki 4a-4g.**

§ 6

Środki organizacyjne ochrony danych osobowych

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne:

a/. Przetwarzanie danych osobowych przez Administratora może odbywać się wyłącznie w ramach wykonywania powierzonych zadań przez osoby uprawnione. Zakres uprawnień wynika z zakresu tych zadań.

b/. Do przetwarzania danych w systemie informatycznym lub w wersji papierowej mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi **załącznik nr 5,**

c/. Przedmiotowe upoważnienie nadawane jest w formie papierowej, indywidualnie, w zakresie zgodnym z zakresem obowiązków danego pracownika.

2. Upoważnienia są wydawane według poniższych zasad;

a/. osoba na stanowisku ds. kadr przygotowuje dwa egzemplarze upoważnienia dla osoby do przetwarzania danych osobowych,

b/. Administrator lub osoba upoważniona podpisuje upoważnienie,

c/. osoba na stanowisku ds. kadr aktualizuje na bieżąco osoby upoważnione do przetwarzania danych osobowych,

d/. jeden egzemplarz upoważnienia do przetwarzania danych osobowych otrzymuje osoba upoważniona do przetwarzania danych osobowych, drugi egzemplarz przechowywany jest przez pracownika ds. kadr wraz z innymi upoważnieniami.

3. Powierzenia przetwarzania danych osobowych innemu podmiotowi jest możliwe wyłącznie na podstawie umowy zawartej w formie pisemnej przez Administratora z podmiotem przetwarzającym. Umowa winna spełniać wymagania o których mowa w art.28 rozporządzenia. Wzór umowy stanowi **załącznik nr 6.**

4. Administrator prowadzi ewidencję umów powierzenia według wzoru stanowiącego **załącznik nr 7.**

§ 7

Udostępnianie danych osobowych

Zasady obowiązujące przy udostępnianiu danych osobowych;

1. Do udostępniania danych osobowych zgromadzonych w zbiorach upoważniony jest Nadleśniczy lub osoba upoważniona.

2. Administrator udostępnia dane osobowe zgromadzone w zbiorach osobom lub podmiotom uprawnionym wyłącznie na pisemny umotywowany wniosek.
3. Udostępnienia danych osobowych muszą być ewidencjonowane. Wzór rejestru stanowi **załącznik nr 8.**

Procedura przekazywania danych osobowych;
1. Podczas przekazywania dane muszą być zabezpieczone przez nieuprawnionym dostępem.
2. Dane przesyłane drogą teleinformatyczną muszą być odpowiednio zabezpieczone przed utratą ich poufności i integralności za pomocą zabezpieczeń kryptograficznych zapewniających ich bezpieczne przesyłanie.

§ 8

Rejestr czynności przetwarzania danych osobowych

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, który zawiera następujące informacje;
a/. nazwę Administratora oraz dane kontaktowe,
b/. cele przetwarzania,
c/. opis kategorii osób oraz kategorii danych osobowych,
d/. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych,
e/. w przypadku gdy ma to zastosowanie, przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
f/. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych danych osobowych,
g/. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa o których mowa w art.32 ust.1 Rozporządzenia.
2. W rejestrze można podać dodatkowe, inne informacje.
3. Rejestr jest prowadzony w formie pisemnej oraz elektronicznej.
4. Wzór rejestru stanowi **załącznik nr 9.**

§ 9

Przetwarzanie danych osobowych

1. Przetwarzanie danych osobowych na komputerze może odbywać się wyłącznie w miejscach do tego wyznaczonych. Każdy pracownik posiada przydzielone miejsce pracy.
2. Na każdym użytkowniku komputera spoczywa odpowiedzialność za rodzaj i zakres danych przetwarzanych przez niego w ramach przydzielonych mu uprawnień oraz odpowiedzialność za ochronę tych danych przed dostępem osób nieuprawnionych, nieuprawnioną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

ROZDZIAŁ IV

Zakres czynności Administratora Systemu Informatycznego w Nadleśnictwie

§ 1

Administrator Systemu Informatycznego, którym w Nadleśnictwie Opole jest Pan Rafał Miłkowski i Pan Mariusz Kurek.

1. zarządza systemem informatycznym Administratora, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych na poziomie administratora,
2. dokonuje zgłoszenia do zarejestrowania użytkownika w systemie informatycznym w związku z zatrudnieniem pracownika oraz dokonuje odbioru uprawnień do systemów informatycznych w przypadku ustania zatrudnienia.
3. zapobiega dostępowi do systemu informatycznego przez osoby nieuprawnione,
4. przygotowuje do akceptacji uprawnienia w systemach informatycznych upoważnionym pracownikom zgodnie ze wskazaniem ich przełożonych,
5. wykonuje samodzielnie lub z udziałem podmiotów uprawnionych audyt legalności zainstalowanego oprogramowania na komputerach użytkowanych przez pracowników,
6. w przypadku stwierdzenia naruszenia zabezpieczeń systemu informatycznego lub użytkowania nielegalnego oprogramowania informuje o powyższym Administratora i współdziała przy usuwaniu skutków naruszenia,
7. inicjuje i nadzoruje wdrażanie nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mogą doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
8. informuje Administratora o konieczności wprowadzenia zmian w Polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym pod kątem spraw informatycznych.

ROZDZIAŁ V

Instrukcja zarządzania systemem informatycznym

§ 1

Procedura nadawania i rejestrowania uprawnień do przetwarzania danych osobowych

1. Stosowane są dwa rodzaje uprawnień dostępu;
a/. do poziomu domeny (systemu operacyjnego Windows oraz konta pocztowego),
b/. do poziomu systemów informatycznych (głownie do systemu SILP).
2. Nadawanie i odbieranie uprawnień dostępu do systemów informatycznych o których mowa w pkt. 1 lit. b wykonuje ASI na podstawie otrzymanej informacji od bezpośredniego przełożonego danego pracownika o zakresie udzielonego lub odebranego dostępu.
3. Dostęp do systemów informatycznych, jest zatwierdzany przez Administratora.
4. Wykaz nadanych uprawnień rejestrowany jest w formie elektronicznej w aplikacji silp-web.
5. Identyfikacja w systemie informatycznym odbywa się po uprzedniej weryfikacji

indywidualnego loginu i hasła lub identyfikatora i hasła danego pracownika.
6. Procedura wyrejestrowywania użytkownika;
a/. pracownik zajmujący stanowisko specjalisty ds. pracowniczych jest zobowiązany do niezwłocznego powiadomienia ASI o ustaniu stosunku pracy z użytkownikiem systemu informatycznego, dokonując jednocześnie aktualizacji ewidencji osób upoważnionych,
b/. ASI dokonuje odbioru uprawnień do systemów o których mowa w pkt. 1. Odbiór uprawnień następuje bez zbędnej zwłoki.

§ 2
Metody i środki uwierzytelniania

1. Dostęp do komputera na którym przetwarzane są dane osobowe musi być zabezpieczony za pomocą mechanizmu; hasło i login.
2. Procedurę zakładania loginów i haseł określają wytyczne i procedury organizacji LP.
3. Zakazuje się udostępniania haseł osobom postronnym.
4. Użytkownikowi nigdy nie wolno zgadzać się na automatyczne zapamiętywanie hasła w systemie komputerowym lub w przeglądarkach.

§ 3
Zasady pracy z pocztą elektroniczną

1. Pracownicy do kontaktów służbowych mogą wykorzystywać wyłącznie służbowe adresy e-mail.
2. Za służbowe adresy e-mail uznaje się takie, które zostały założone w domenie *katowice.lasy.gov.pl* i dostępy do zasobów poczty elektronicznej są kontrolowane (nadawane, blokowane, dobierane) przez RDLP Katowice.
3. Zabroniony jest dostęp do internetu za pośrednictwem łączy, które nie są autoryzowane przez Lasy Państwowe.
4. Zabronione jest przekierowywanie służbowych wiadomości e-mail na prywatne skrzynki mailowe, jak też zapisywanie na prywatne nośniki.
5. Nie jest dopuszczalne przesyłanie na adresy służbowych skrzynek pocztowych wiadomości prywatnych (a zwłaszcza filmów, zdjęć, dokumentów).
6. Każdy użytkownik poczty elektronicznej posiada swoje indywidualne hasło i identyfikator dostępu do konta.
7. Zabronione jest udostępnianie danych do logowania (nazwa konta i haseł).
8. Użytkownik nie ma prawa samodzielnej zmiany konfiguracji stacji roboczych związanych ściśle z przyłączem internetowym.
9. Użytkownicy mają zakaz otwierania podejrzanych e-maili, co oznacza w szczególności, ze nie wolno otwierać wiadomości, które;
a/. pochodzą od osoby nieznanej, która nie ma powodu aby przysyłać wiadomości lub załączniki,
b/. załącznik jest przesyłany w pustej wiadomości,
c/. w e-mailu jest wiadomość ale nie ma jakiegokolwiek sensu,
d/. jest wiadomość, ale wydaje się mało prawdopodobne aby to ten nadawca ją wysłał,
e/. e-mail zawiera łącza do pornograficznych witryn internetowych, erotyczne obrazy, itd.,
f/. wiadomość nie zawiera żadnych osobistych zwrotów (np. wiadomość w której jest

tylko napisane „Musisz na to spojrzeć" lub „Wysyłam to do Ciebie, gdyż potrzebuje twojej porady"),
g/. wiadomość podpisana jest przez nadawcę, którego dane adresowe ze stopki e mail nie odpowiadają danym w domenie, z której e-mail został wysłany,
h/.informacja wskazuje na to, że jest to plik wykonywalny,
i/. załącznik ma nazwę o podwójnym rozszerzeniu np. NAZWA.JPG.vbs lub NAZWA.TXT.scr (podejrzany adresat, temat wiadomości).
10. W przypadku otrzymania podejrzanej wiadomości e-mail lub też w przypadku gdy system antywirusowy/antyspamowy sugeruje, że wiadomość jest niebezpieczna dla systemu, użytkownik ma obowiązek zgłosić sprawę niezwłocznie do ASI.

§ 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

Rozpoczęcie prac;

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje zalogowanie w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione, gdzie bezpośredni dostęp do systemu jest możliwy po podaniu identyfikatora i właściwego hasła.
2. W razie podejrzenia co do możliwości próby włamania do systemu informatycznego, użytkownik zobowiązany jest powiadomić o powyższym bezpośredniego przełożonego.
3. Użytkownik systemu informatycznego jest odpowiedzialny za zabezpieczenie danych wyświetlanych na monitorze przed osobami nie mającymi uprawnień.

Zawieszenie pracy;

1. W przypadku przerwania pracy połączone z opuszczeniem stanowiska oraz pomieszczenia pracy użytkownik zobowiązany jest do zablokowania dostępu do systemu.
2. W przypadku udostępnienia stanowiska pracy innej osobie, użytkownik musi wylogować się z systemu.

Zakończenie pracy;

1. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.
2. Użytkownik opuszczający stanowisko pracy musi zabezpieczyć komputer przed dostępem osób trzecich.
3. Wyłączenie komputera może nastąpić tylko po wcześniejszym zamknięciu wszystkich włączonych programów.
4. Zabrania się wyłączać komputer w czasie działania programów.

§ 5

Tworzenia kopii zapasowych

1. Kopia bezpieczeństwa sporządzonych dokumentów, poczty e-mail wykonywana jest automatycznie i archiwizowana na macierzy.
2. Zabrania się wykonywania kopii plików zawierających dane osobowe na innych urządzeniach i nośnikach.

§ 6

Przechowywanie elektronicznych nośników informacji

Dane osobowe w formie elektronicznej przechowywane są na serwerach obsługujących system informatyczny Administratora, a także innych dopuszczonych w Lasach Państwowych formach, w tym dyskach lokalnych komputerów w lokalizacji ustalonej z Administratorem. Zabrania się gromadzenia danych osobowych na innych, nieautoryzowanych nośnikach danych.

§ 7

Zabezpieczenie systemu informatycznego przed złośliwym oprogramowaniem

1. Administrator zapewnia ochronę antywirusową.
2. Za instalację programu antywirusowego odpowiedzialny jest ASI.
3. Na styku sieci wewnętrznej z siecią publiczną został zainstalowany firewall.
4. W przypadkach wykrycia infekcji przez program antywirusowy, użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.
5. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia.

§ 8

Praca na urządzeniach przenośnych

1. Użytkownik, któremu powierzono urządzenie przenośne powinien chronić je przez uszkodzeniem, zniszczeniem, kradzieżą oraz dostępem osób nieuprawnionych. Zachowanie szczególnej ostrożności wymagane jest podczas transportu.
2. Użytkownik nie ma prawa udostępniać urządzenia przenośnego do korzystania osobom trzecim, w tym także zabezpieczyć je przed możliwością włączenia przez osoby nieuprawnione.
3. ASI na bieżąco z wykorzystaniem podmiotów uprawnionych dokona zaszyfrowania dysków.
4. Zabrania się pozostawiania urządzeń przenośnych bez opieki w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nim skutecznego nadzoru.
5. W przypadku utraty urządzenia przenośnego użytkownik niezwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego, a w przypadku kradzieży dokonuje również niezwłocznego zgłoszenia faktu popełnienia przestępstwa na Policji. W zawiadomieniu użytkownik, poza danymi ogólnymi, podaje okoliczności utraty urządzenia przenośnego oraz opis charakteru utraconych danych wraz z podaniem ich znaczenia. W szczególności w zawiadomieniu należy określić, czy utracone dane miały charakter danych osobowych.

§ 9

Zasady odpowiedzialności użytkownika

1. Sprzęt komputerowy (laptop) może być wynoszony poza teren Nadleśnictwa wyłącznie po uzyskaniu zgody Administratora.
2. Zasady i procedury przewidziane w Polityce bezpieczeństwa i instrukcja zarządzania systemem informatycznym obowiązują każdego pracownika Administratora oraz innych użytkowników (np. stażyści, praktykanci), którzy mają dostęp do przetwarzania danych osobowych u Administratora.

3. Każdy pracownik jest odpowiedzialny indywidualnie za powierzony sprzęt w tym za ujemne następstwa korzystania ze sprzętu przez osobę nieuprawnioną, któremu udostępnił sprzęt.
4. Utrata lub kradzież sprzętu winna być niezwłocznie zgłaszana bezpośredniemu przełożonemu, który powiadamia ASI oraz Administratora.
5. Wszelkie instalacje oprogramowania mogą być dokonywane wyłącznie przez ASI.
6. Brak stosowania się przez pracowników do zasad i procedur przewidzianych w Polityce bezpieczeństwa i instrukcja zarządzania systemem informatycznym może być potraktowane jako naruszenie obowiązków pracowniczych.

§ 10
Przesyłanie danych

1. Informacje zawierające dane osobowe mogą być przekazywane za pomocą łączy internetowych w sposób zapewniający poufność i integralność tych danych, np. zaszyfrowanie.
2. W wypadku przesyłania danych osobowych przez sieć internetową pocztą elektroniczną dopuszcza się zabezpieczenie załączników ochroną kryptologiczną poprzez nadanie hasła odczytu. W przypadku nadania hasła, należy je przesłać lub podać odbiorcy w innej przesyłce, a najlepiej z wykorzystaniem innych metod komunikacji (telefon, fax, w bezpośredniej rozmowie). Tym samym haseł dostępu, czy kluczy aktywacyjnych do danych nie można przekazywać tą samą drogą, co dane. Powyższe nie dotyczy przesyłania pocztą elektroniczną wewnątrz Lasów Państwowych, czyli w sieci WAN LP.

§ 11
Wykonywanie przeglądów, konserwacji systemów oraz nośników informacji

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie ASI. Stwierdzone nieprawidłowości w funkcjonowaniu sprzętu lub działaniu programów służących do przetwarzania danych osobowych, usuwa się niezwłocznie.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego nieupoważnionych.
3. W przypadku konieczności przeprowadzenia prac serwisowych w serwisie zewnętrznym lub osobą nie posiadają uprawnień do przetwarzania danych osobowych, ASI zobowiązany jest do odpowiedniego zabezpieczenia danych znajdujących się na dyskach urządzenia. Jeżeli nie jest możliwe odpowiednie zabezpieczenie danych na dyskach, wszelkie naprawy muszą być wykonane w obecności ASI.
4. Likwidację nośnika informacji zawierającego dane osobowe należy przeprowadzić poprzez firmy wyspecjalizowane w profesjonalnym niszczeniu dysków twardych oraz danych zapisanych na innych nowoczesnych, elektronicznych nośnikach.

§ 12
Wytyczne dotyczące wewnętrznych okresów przechowywania

1. Każdy pracownik zobowiązany jest do stosowania się do zasady ograniczenia czasowego przetwarzania danych osobowych. Oznacza to, że dane osobowe mogą

być przechowywane w formie umożliwiającej identyfikacje osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
2. Wymaga się zapewnienia okresu ograniczenia przechowywania danych do ścisłego minimum.
3. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne stosuje się przepisy wewnętrzne obowiązujące w Lasach Państwowych, po czym dane powinny zostać usunięte lub zanonimizowane.
4. Bez względu na powyższe każdy pracownik zobowiązany jest do okresowego przeglądu danych osobowych, na których pracuje pod kątem ich przydatności.
5. W przypadku zidentyfikowania niepotrzebnych plików/dokumentów/wiadomości – powinny one zostać niezwłocznie w sposób trwały usunięte przez pracownika.
6. Do czasu ich usunięcia dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

§ 13

Procedura postępowania w sytuacji naruszeń ochrony danych osobowych

Poniżej zdefiniowano możliwe naruszenia oraz opisano zasady postępowania w przypadku ich wystąpienia, jak również działania celem ograniczenia możliwości ich występowania w przyszłości.

Zasady postępowania:

1. W przypadku stwierdzenia naruszenia (tj. zabezpieczenia systemu informatycznego, stanu technicznego urządzeń, zawartości zbiorów danych osobowych, ujawnienia metody pracy lub sposobu działania programu, jakości transmisji danych w sieci telekomunikacyjnej, mogącej wpływać na naruszenie zabezpieczeń tych danych, innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych), każdy pracownik Administratora obowiązany jest niezwłocznie o powyższym fakcie poinformować IOD, a w razie niemożności zawiadomienia IOD należy powiadomić bezpośredniego przełożonego.
2. Pracownik w przypadku stwierdzenia zaistnienia okoliczności wskazanych w ust.1 do czasu spełnienia przesłanki w nim określonym zobowiązany jest;
a/. zabezpieczyć ślady naruszenia,
b/. zapobiec dalszym zagrożeniom,
c/. podjąć czynności niezbędne do powstrzymywania niepożądanych skutków naruszenia,
d/. ustalić (jeżeli jest to możliwe) przyczyny i sprawców naruszenia,
e/. rozważyć czasowe wstrzymanie pracy na komputerze w celu zabezpieczenia miejsca zdarzenia,
f/. zaniechać (o ile jest to możliwe) dalszych działań, które wiążą się z zaistniałym zdarzeniem, a które mogą utrudnić jego udokumentowanie i analizę,

g/. podjąć stosowne działania przewidziane w obowiązujących przepisach (w tym instrukcjach) przy uwzględnieniu komunikatów jakie pojawiają się w związku z naruszeniem,
h/. przygotowania (udokumentowania wstępie) opisu zdarzenia,
i/. pozostać na miejscu zdarzenia do czasu przybycia osoby upoważnionej.
3. IOD lub osoba upoważniona po przybyciu na miejsce zdarzenia powinna niezwłocznie;
a/. przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia bezpieczeństwa danych osobowych,
b/. podjąć działania (w tym dokonać wyboru dalszego postępowania) z punktu widzenia ewentualnego zagrożenia dla prawidłowości pracy i funkcjonowania Administratora,
c/. podjąć inne, uzasadnione w jego ocenie działania w sprawie.
4. Z chwilą przywrócenia stanu istniejącego przed zdarzeniem należy dokonać wnikliwej analizy w celu ustalenia przyczyn naruszenia oraz podjąć działania celem wyeliminowania podobnych zdarzeń w przyszłości oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości;
a/. jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych,
b/. jeżeli przyczyną było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe,
c/. jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje zgodnie z przepisami,
d/. jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożenia środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych,
e/. jeżeli przyczyną zdarzenia był zły stan techniczny urządzeń lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrole czynności serwisowo-programowych.
5. IOD dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który zawiera w szczególności;
a/. wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub rozpytanych w związku z naruszeniem,
b/. określenie czasu i miejsca naruszenia oraz powiadomienia,
c/. określenie okoliczności towarzyszących i rodzaju naruszenia,
d/. wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
e/. wstępną ocenę przyczyn wystąpienia naruszenia,
f/. ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego,
g/. decyzję co do zgłoszenia naruszenia do Organu Nadzorczego oraz jej uzasadnienie,
h/. decyzję co do poinformowania osób, których dane dotyczą i jej uzasadnienie.

Raport o którym mowa powyżej IOD niezwłocznie przekazuje Administratorowi, a w przypadku jego nieobecności osobie uprawnionej.
6. Po wyczerpaniu środków doraźnych po zaistniałym zdarzeniu IOD zasięga niezbędnych opinii i proponuje postępowania naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
7. Zaistniałe naruszenie może być przedmiotem szczegółowej, zespołowej analizy przeprowadzonej przez kierownictwo Administratora, IOD oraz osoby zainteresowane. Analiza ta powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.
8. Po zapoznaniu się z opisem zdarzenia, Nadleśniczy podejmuje decyzję o dalszym trybie postępowania, ewentualnym powiadomieniu Organu Nadzorczego oraz, jeśli to konieczne osoby/osób, których dane dotyczą.
9. Zawiadomienie organu nadzorczego musi nastąpić bez zbędnej zwłoki – w miarę możliwości, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
10. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
11. Zgłoszenie do Organu Nadzorczego musi co najmniej;
a/. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną ilość osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
b/. zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
c/. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
d/. opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzeniu naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
12. IOD lub osoba upoważniona dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania. Powyższe zawiera analiza z naruszenia ochrony danych osobowych według wzoru stanowiącego **załącznik nr 10.** Wszystkie analizy są ewidencjonowane. Zbiorem ewidencji naruszeń jest zbiór analiz o których mowa powyżej.
13. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu. Zawiadomienie to musi zostać sformułowane jasnym i prostym językiem i opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej:

a/. nazwę oraz dane kontaktowe Administratora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
b/. wskazywać możliwe konsekwencje naruszenia ochrony danych osobowych,
c/. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
14. Zawiadomienie o którym mowa w pkt. 13 nie jest wymagane w następujących przypadkach:
a/. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające osobom nieuprawnionym dostęp do tych danych osobowych,
b/. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
c/. wymagałoby one niewspółmiernie dużego wysiłku. W takim wypadku zostaje wydany publiczny komunikat lub zostaje zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą zostają poinformowane w równie skuteczny sposób.
15. Każdy pracownik Administratora jest zobowiązany do niezwłocznego poinformowania bezpośredniego przełożonego, IOD oraz w przypadku danych osobowych przetwarzanych z użyciem systemu informatycznego służącego do przetwarzania danych osobowych – ASI, o każdym przypadku złamania zasad przetwarzania danych, a w szczególności o sytuacjach ujawnienia danych osobom nieuprawnionym.

ROZDZIAŁ VI

ANALIZA RYZYKA OGÓLNEGO I OCENY SKUTKÓW dla PRZETWARZANIA DANYCH (DPIA)

WSTĘP

Mając na względzie konieczność uwzględnienia w procesie przetwarzania danych osobowych prawdopodobieństwa i powagi ryzyka naruszeń praw lub wolności osób, których przetwarzanie dotyczy, Administrator wprowadza do organizacji procedurę szacowania ryzyka w stosunku do aktualnie prowadzonych jak i planowanych operacji przetwarzania danych osobowych.

§1
Cel szacowania ryzyka

1. Administrator przeprowadza proces szacowania ryzyka w zakresie bezpieczeństwa informacji w celu zidentyfikowania obszarów, które mogą istotnie

wpływać na osobę, której przetwarzanie dotyczy. Administrator wdraża podejście oparte na ryzyku, aby zapewnić ochronę praw i wolności osób, których przetwarzanie dotyczy.

2. Na szacowanie ryzyka składa się;

1/. Analiza Ryzyka Ogólnego,

2/. Ocena Skutków dla Przetwarzania Danych (DPIA).

§2

Definicje legalne

Ilekroć w „Analizie Ryzyka Ogólnego i Ocenie Skutków dla Przetwarzania Danych (DPIA)" mówi się o;

1. „szacowaniu ryzyka" – należy przez to rozumieć proces analizy i oceny ryzyka. W procesie szacowania ryzyka w kontekście danych osobowych szacowanie ryzyka uwzględnia ryzyko związane z naruszeniem praw i wolności osób fizycznych, których przetwarzanie dotyczy,

2. „analizie ryzyka" – należy przez to rozumieć proces identyfikacji źródeł ryzyka i oszacowania ryzyka,

3. „ocenie ryzyka" – należy przez to rozumieć proces porównywania oszacowanego ryzyka w celu określenia znaczenia ryzyka,

4. „ryzyku" – należy przez to rozumieć kombinacje prawdopodobieństwa zdarzenia i jego konsekwencji,

5. „ryzyku szczątkowym" – należy przez to rozumieć ryzyko pozostające po procesie postępowania z ryzykiem,

6. „postępowaniu z ryzykiem" – należy przez to rozumieć proces zmiany poziomu ryzyka poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych,

7. „akceptacji ryzyka" – należy przez to rozumieć decyzje Administratora o tym, aby ryzyko zaakceptować,

8. „podatności" – należy przez to rozumieć słabość w strukturze fizyczne, technicznej, organizacyjnej nadleśnictwa.

9. „incydencie" – należy przez to rozumieć zdarzenie mające lub mogące mieć negatywny wpływ na System Zarządzania Bezpieczeństwem Informacji w nadleśnictwie. Incydent może powodować w stosunku do osoby fizycznej, której dane osobowe nadleśnictwa przetwarza, szkodę o charakterze majątkowym lub niemajątkowym,

10. „poufności" – należy przez to rozumieć właściwość polegająca na tym, że osoba nieupoważniona bądź podmiot nie mają dostępu do danych osobowych, które temu atrybutowi podlegają,

11. „integralności" – należy przez to rozumieć właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają kompletne,

12. „dostępności" – należy przez to rozumieć właściwość polegającą na tym, że aktywna w postaci informacji/danych osobowych pozostają dostępne dla osób upoważnionych/uprawnionych do ich przetwarzania,

13. „bezpieczeństwie informacji" – należy przez to rozumieć zachowanie wobec

przetwarzanych danych osobowych/informacji takich atrybutów jak poufność, integralność oraz dostępność.

§3

Oznaczenie uwarunkowań związanych z funkcjonowaniem nadleśnictwa – ustalenie kontekstu

1. Nadleśnictwo określa, które z uwarunkowań zewnętrznych bądź wewnętrznych mają znaczenie dla szacowania ryzyka.
2. Uwarunkowania zewnętrzne istotnie wpływające na nadleśnictwo;
   1/. Relacje z innymi administratorami danych osobowych,
   2/. Relacje z innymi podmiotami zewnętrznymi,
   3/. Zasięg terytorialny działalności nadleśnictwa,
   4/. Uwarunkowania prawne organizacyjne.
3. Uwarunkowania wewnętrzne istotnie wpływające na nadleśnictwo;
   1/. Struktura i rozmiar nadleśnictwa,
   2/. Uwarunkowania formalne wewnętrzne (regulaminy),
   3/. Sposób podejmowania decyzji w nadleśnictwie względem bezpieczeństwa przepływu danych,
   4/. Kultura nadleśnictwa.
4. Nadleśnictwo na etapie tworzenia Polityki Bezpieczeństwa i instrukcji zarządzania systemem informatycznym przeanalizowało;
   1/. Postawy legalności przetwarzania danych (w oparciu o przesłanki wynikające z RODO),
   2/. Staranność po stronie nadleśnictwa w zakresie spełniania obowiązków informacyjnych oraz realizacji praw osób fizycznych, których dane osobowe dotyczą w oparciu o RODO,
   3/. Cel przetwarzania danych osobowych, chyba, że nadleśnictwo działa w imieniu innego administratora (w procesie przetwarzania danych nadleśnictwo działa w roli procesora),
   4/. Zakres przetwarzania danych kierując się zasadami przetwarzania danych określonymi w RODO,
   5/. Wymagania dotyczące zabezpieczeń nadleśnictwa, środków kontroli logicznej procesu przetwarzania, środków ochrony fizycznej danych.

§4

Wybór metod na cele przeprowadzania Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania Danych (DPIA)

1. Rozporządzenie pozostawia Administratorowi wybór w zakresie zastosowania konkretnej metody szacowania ryzyka.
2. Administrator ma świadomość, iż w procesie szacowania ryzyka może kierować się metodą;
   1/. ilościową; wielkość poniesionych strat próbuje się wyrazić liczbowo,

niejednokrotnie w oparciu o dane statystyczne, bądź,

2/. jakościową; wielkość zagrożenia ocenia się przez pryzmat doświadczenia oraz intuicji osoby szacującej ryzyko (subiektywne odczucie).

3. Administrator ma świadomość, iż szacowanie ryzyka w procesie przetwarzania danych osobowych powinno opierać się o metodą jakościową – strat związanych z ochroną danych osobowych bardzo często nie sposób wyrazić za pomocą liczb.

4. Atrybuty, jakie Administrator przyjmuje w tabeli szacowania ryzyka, to;

1/. Poufność – osoba nieupoważniona bądź nieupoważniony podmiot nie mają dostępu do danych osobowych. Dane osobowe zgodnie z tym atrybutem nie są ujawniane w nieuprawniony sposób.

2/. Integralność – konieczność zapewnienia spójności danych osobowych; atrybut determinujący konieczność ochrony danych osobowych przed przypadkowym ich zniekształceniem w przypadku ich zapisu, odczytu, transmisji bądź magazynowania,

3/. Dostępność – zasób w postaci danych osobowych jest możliwy do wykorzystania na żądanie w konkretnym czasie przez osobę bądź podmiot upoważniony/uprawniony w zakresie dostępu do danych.

§5

Klasyfikacja czynności przetwarzania

1. Administrator w pierwszej kolejności dzieli czynność przetwarzania na te, które wymagają Oceny Skutków dla Przetwarzania Danych (DPIA) oraz te, względem których Administrator wykonuje Analizę Ryzyka Ogólnego.

2. Kryterium, według którego Administrator dokonuje wstępnej klasyfikacji z uwzględnieniem kontekstu przetwarzania danych są wytyczne Grupy Roboczej art. 29WP 248 rew. 01 17/PL dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679;

1/. Ocena lub punktacja; w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" (motyw 71 i 91),

2/. automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku; przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „ w podobny sposób istotnie na nie wpływają (art. 35 ust.3 lit.a)). Zagrożenie; przetwarzanie mogące prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie mające niewielki wpływ na osoby fizyczne lub niemające na nie żadnego wpływu nie spełnia tego konkretnego kryterium.

3/. Systematyczne monitorowanie; przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub w ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust.3 lit.c)). Zagrożenie; osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich

dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub przestrzeni publicznie dostępnej).

4/. Dane wrażliwe lub dane o charakterze wysoce osobistym; obejmują szczególne kategorie danych osobowych określonych w art. 9 oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszenia prawa zdefiniowane w art. 10,

5/. Dane przetwarzane na dużą skalę; przy ustaleniu, czy przetwarzanie odbywa się na dużą skalę, Administrator bierze pod uwagę następujące czynniki;

a/. liczbę osób, których dane dotyczą – wyrażona jako konkretna wartość albo jako odsetek populacji odniesienia,

b/. ilość danych lub zakres poszczególnych przetwarzanych pozycji danych,

c/. czas trwania lub trwałość czynności przetwarzania danych,

d/.zakres geograficzny czynności przetwarzania.

6/. Dopasowanie lub łączenie zbiorów danych; zbiory pochodzące co najmniej z dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą,

7/. Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą; przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych osobowych lub z wyrażeniem sprzeciwu wobec ich przetwarzania lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki , których dane dotyczą, zalicza się dzieci, pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony oraz w każdą sytuację, gdzie można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.

8/. Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych, takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu. Zastosowanie takiej technologii może się wiązać z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. Ocena skutków dla ochrony tych danych pomoże Administratorowi zrozumieć ryzyko i je wyeliminować,

9/. Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie praw i korzystanie z usług lub umowy". Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usług lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

3. Powyższe wytyczne znajdują źródło w art. 35 ust.3 RODO;

„Ocena skutków dla danych osobowych, o której mowa w ust.1, jest wymagana w szczególności w przypadku;

a/. systematyczne, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym

profilowaniu i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną.
b/. przetwarzanie na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust.1 lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
c/. systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie.
4. Administrator przyjmuje zasadę, że przetwarzanie spełniające dwa kryteria, będzie skutkowało koniecznością przeprowadzenia Oceny Skutków dla Przetwarzania Danych (DPIA).
5. Administrator może uznać, iż przetwarzanie wyczerpujące tylko jedno z przywołanych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych.
6. Administrator może równocześnie stwierdzić, iż przetwarzanie wyczerpuje więcej niż dwa kryteria, ale mimo to nie przeprowadza oceny skutków dla ochrony danych. W takim przypadku Administrator uzasadnia i dokumentuje powody, dla których nie przeprowadzono oceny skutków dla ochrony danych.
7. Ocena Skutków dla Przetwarzania Danych (DPIA) nie jest obowiązkowa w przypadku;
1/. Gdy nie jest prawdopodobne, aby operacja przetwarzania może powodować wysokie ryzyko,
2/. Gdy przetwarzano już podobną ocenę skutków dla ochrony danych,
3/. Gdy operacja przetwarzania posiada podstawę prawną, która reguluje dana operacje przetwarzania.
4/. Gdy operacja przetwarzania znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych.

§6
Grupowanie podobnych czynności przetwarzania

1. Zgodnie z art. 35 ust.1 RODO dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem Administrator przeprowadza pojedynczą ocenę.
2. Administrator grupuje podobne operacje przetwarzania dla Analizy ryzyka ogólnego (ARO) oraz Oceny Skutków Przetwarzania Danych (DPIA) uwzględniając kontekst ich przetwarzania w oparciu o następujące kryteria;
1/. ARO-Gr 1- dane osobowe związane pracownikami.
2/. ARO-Gr 2 – dane osobowe związane z usługami „na zewnątrz" (np. usługobiorcy).
3/. ARIO-GR 3- dane osobowe związane z usługami „do wewnątrz" (np. kontrahenci, usługodawcy),
4/. DPIA-Gr 1 – dane osobowe związane z pracownikami
5/. DPIA-GR 2 – dane osobowe związane z usługami „ na zewnątrz"

§7
Szacowanie ryzyka

1. Proces szacowania ryzyka Administrator poprzedza identyfikacją aktów nadleśnictwa, zagrożeń dla aktywów, zabezpieczeń stosowanych w nadleśnictwie, podatności (prawdopodobieństwa) oraz następstw (skutków).
2. Nadleśnictwo identyfikuje aktywna i dzieli je na aktywa podstawowe i aktywa wspierające.
1/. Do aktywów podstawowych nadleśnictwo zalicza;
a/. informacje – obejmują dane osobowe, które nadleśnictwo przetwarza w związku z prowadzoną działalnością, informacje niezbędne do osiągnięcia celów nadleśnictwa.
b/. operacja przetwarzania czynności w procesie przetwarzania danych osobowych, które nadleśnictwo jest zobowiązane podejmować/utrzymywać aby osiągnąć cele strategiczne przy jednoczesnym zapewnieniu bezpieczeństwa przetwarzania informacji w nadleśnictwie.
2/. Do aktywów wspierających nadleśnictwo zalicza;
a/. sprzęt – obejmuje przenośne urządzenia komputerowe, urządzenia serwerowe, urządzenia peryferyjne (drukarki, czy wymienny napęd dyskowy),
b/. nośniki danych (papierowe) zawierające dane osobowe – dokumentacja zawierająca treści o charakterze osobowym,
c/. nośniki danych elektroniczne – z racji swojego przeznaczenia mogą być podłączone do urządzenia komputerowego w celu przygotowania danych osobowych do przetworzenia (płyta CD ROM, wymienny dysk twardy),
d/. oprogramowanie – obejmuje wszystkie programy dzięki którym bądź w oparciu o nie nadleśnictwo przetwarza dane osobowe. W zakresie oprogramowania uwzględnia się system operacyjny, oprogramowanie uzupełniające usługi systemu operacyjnego, oprogramowanie służące do obsługi poczty elektronicznej czy bazy danych, standardowe i dedykowane aplikacje biznesowe np. oprogramowanie księgowe, służące do obsługi klientów, pracowników nadleśnictwa.
e/. okablowanie - sieć, którą należy rozumieć przez pryzmat urządzenia używanego do połączenia wielu komputerów i elementów systemu informacyjnego.
f/. personel – osoby zaangażowane w proces przetwarzania danych osobowych oraz obsługę systemu informacyjnego. Do personelu zaliczany kierownictwo, osoby upoważnione do przetwarzania danych, osoby, które mają w zakresie swoich obowiązków m.in. konieczność utrzymania systemu informacyjnego.
g/. lokalizację – siedziba ale również środowisko zewnętrzne. Siedziba nadleśnictwa odnosi się do budynku/budynków jakie nadleśnictwo zajmuje oraz wszystkich obszarów przetwarzania wewnątrz budynków. Siedziba jest istotna ze względu na jej położenie geograficzne, obszar miejski, przestrzeń publiczną.
3. Nadleśnictwo identyfikuje zagrożenia i dzieli je na;
1/. Zniszczenia fizyczne;
a/. pożar,
b/. zalanie,

c/. zanieczyszczenie,
d/. poważny wypadek,
e/. zniszczenie urządzeń lub nośników,
f/. pył, korozja, wychłodzenie,
2/. Zjawiska naturalne;
a/. zjawiska klimatyczne,
b/. zjawiska sejsmiczne,
c/. zjawiska wulkaniczne,
d/. zjawiska pogodowe,
e/. powódź.
3/. Utrata podstawowych usług;
a/. awaria systemu klimatycznego lub dostaw wody,
b/. utrata dostaw prądu,
c/. awaria urządzenia telekomunikacyjnego.
4/. Zakłócenia spowodowane promieniowaniem;
a/. promieniowanie elektromagnetyczne,
b/. promieniowanie cieplne,
c/. impuls elektromagnetyczny.
5/. Naruszenie bezpieczeństwa informacji;
a/. przechwycenie sygnałów na skutek zjawiska interferencji,
b/. szpiegostwo zdalne,
c/. podsłuch,
d/. kradzież nośników lub dokumentów,
e/. kradzież urządzenia,
f/. odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników,
g/. ujawnienie,
h/. dane z niewiarygodnych źródeł,
i/. manipulowanie urządzeniem,
j/. sfałszowanie oprogramowania,
k/. detekcja umiejscowienia.
6/. Awaria techniczna;
a/. awaria urządzenia,
b/ niewłaściwe funkcjonowanie urządzeń,
c/. przeciążenie systemu informacyjnego,
d/. niewłaściwe funkcjonowanie oprogramowania,
e/. naruszenie zdolności systemu informacyjnego.
7/. Nieautoryzowane działania;
a/. nieautoryzowane użycie urządzeń,
b/. nieuprawnione kopiowanie oprogramowania,
c/. użycie fałszywego lub skopiowanego oprogramowania,
d/. nielegalne przetwarzanie danych.
8/. Naruszenie bezpieczeństwa funkcji;
a/. błąd użytkowania,
b/. naruszenie praw,

c/. fałszowanie praw,
d/. odmowa działania,
e/. naruszenie dostępności personelu.

4. Organizacja identyfikacji podatności (prawdopodobieństwo) wystąpienia zdarzenia w nadleśnictwie zgodnie z poniższą skalą;

PRAWDOPODOBIEŃSTWO	SKALA	CZĘSTOTLIWOŚĆ WYSTĄPIENIA ZDARZENIA
Zdarzenie niemal pewne	4	Zdarzenie występujące co najmniej raz w tygodniu
Zdarzenie wysoce prawdopodobne	3	Zdarzenie występujące co najmniej raz w miesiącu
Zdarzenie mało prawdopodobne	2	Zdarzenie występujące co najmniej raz na kwartał
Zdarzenie nieprawdopodobne	1	Zdarzenie występujące co najmniej raz w roku

5. Nadleśnictwo identyfikuje skutek wystąpienia zdarzenia w nadleśnictwie zgodnie z poniższą skalą;

SKUTEK	SKALA	OPIS NASTĘPSTW
Zdarzenie wywołujące katastrofalny skutek	4	- straty finansowe powyżej 100 000 zł dla nadleśnictwa -strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle katastrofalne w skutkach, że powoduje utratę podstawowych potrzeb dla poczucia bezpieczeństwa, - utrata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle katastrofalna w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia) - kara finansowa nałożona przez organ nadzorczy w wysokości 100 000 zł - zakaz przetwarzania danych nałożony decyzja administracyjną przez organ nadzorczy, - strata wizerunkowa nadleśnictwa – brak zaufania ze strony osób, które nadleśnictwo obsługuje w ramach wykonywanej działalności - orzeczenie wyroku

		skazującego w zakresie przetwarzania danych przez nadleśnictwo
Zdarzenie wywołujące bardzo znaczący skutek	3	- straty finansowe powyżej 50 000 zł dla nadleśnictwa - strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znaczące w skutkach, że powoduje utratę podstawowych potrzeb dla poczucia bezpieczeństwa, - utrata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę uznania . (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), - kara finansowa nałożona przez organ nadzorczy w wysokości 50 000 zł - zakaz przetwarzania danych nałożony decyzja administracyjną przez organ nadzorczy, - strata wizerunkowa nadleśnictwa – brak zaufania ze strony osób, które nadleśnictwo obsługuje w ramach wykonywanej działalności
Zdarzenie wywołujące znaczący skutek	2	- straty finansowe powyżej 3000 zł dla nadleśnictwa - strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę podstawowych potrzeb dla poczucia bezpieczeństwa, - utrata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle katastrofalna w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia) - kara finansowa nałożona przez organ nadzorczy w wysokości 3000 zł - zakaz przetwarzania danych nałożony decyzja administracyjną przez organ nadzorczy,

		- strata wizerunkowa nadleśnictwa – brak zaufania ze strony osób, które nadleśnictwo obsługuje w ramach wykonywanej działalności
Zdarzenie wywołujące niewielki skutek	1	- straty finansowe poniżej 3000 zł dla nadleśnictwa - strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy wywołuje niewielki skutek, - strata osobista dla osoby fizycznej, której przetwarzanie wywołuje niewielki skutek, - organ nadzorczy daje upomnienie i wzywa do naprawienia braków formalnych (przy założeniu, że nadleśnictwo wypełnia wskazania organu nadzorczego), - skutek nie powoduje utraty zaufania ze strony osób fizycznych, względem których nadleśnictwo wykonuje działalność
Zdarzenie nie powodujące skutku	0	- nie ma straty finansowej, - po stronie osoby fizycznej, której przetwarzanie dotyczy nie występuje ani szkoda o charakterze majątkowym, ani osobistym, - zaufanie osób, które nadleśnictwo obsługuje w ramach działalności nie doznaje żadnego uszczerbku

§8
Dokonanie analizy ryzyka

1. Nadleśnictwo wykorzystuje następujący wzór analizy ryzyka w zakresie wykonywania;
   1/. Analizy Ryzyka Ogólnego,
   2/. Oceny Skutków dla Przetwarzania Danych (DPIA).

WZÓR ANALIZY RYZYKA

R=PXS

WARTOŚĆ	OPIS	ZAKRES
R	poziom wyliczonego ryzyka	xxx
R	wartość przypisana prawdopodobieństwu materializacji zagrożenie niezrealizowania założonych celów przez nadleśnictwo	1 - zdarzenie nieprawdopodobne 2 - zdarzenie mało prawdopodobne 3 - zdarzenie wysoce prawdopodobne 4 - zdarzenie niemal pewne
S	skutki zdarzenia	0 - zdarzenie nie powodujące skutku (nie występuje) 1 - zdarzenie wywołuje niewielki skutek 2 - zdarzenie wywołuje znaczący skutek 3 - zdarzenie wywołuje bardzo znaczący skutek 4 - zdarzenie wywołuje katastrofalny skutek

2. Nadleśnictwo przyjmuje następujący zakres macierzy;

			SKUTEK				
			0	1	2	3	4
PRAWDOPODOBIEŃSTWO	Zdarzenie nieprawdopodobne	1	0	1	2	3	4
	Zdarzenie mało prawdopodobne	2	0	2	4	6	8
	Zdarzenie wysoce prawdopodobne	3	0	3	6	9	12
	Zdarzenie niemal pewne	4	0	4	8	12	16

	Ryzyko niskie
	Ryzyko średnie
	Ryzyko wysokie

3. Nadleśnictwo przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Analizy Ryzyka Ogólnego;

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowanego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzje w zakresie; - obniżenia ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych, - pozostawienie ryzyka i niepodejmowanie dalszych działań, - unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka, - przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany - działanie może zostać przesunięte w czasie, nie wymaga określonego monitorowania.
Ryzyko WYSOKIE	od 12 do 16	Poziom ryzyka nieakceptowany - wymaga bezwzględnej reakcji - cel; zredukowanie podatności

4. Nadleśnictwo przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Oceny Skutków dla Przetwarzania Danych (DPIA);

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowanego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzje w zakresie; - obniżenia ryzyka poprzez wdrażanie odpowiednich środków technicznych

		i organizacyjnych, - pozostawienie ryzyka i niepodejmowanie dalszych działań, - unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka, - przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany - działanie może zostać przesunięte w czasie, nie wymaga określonego monitorowania.
Ryzyko WYSOKIE	od 12 do 16	Wymaga bezwzględnej reakcji - cel; zredukowanie podatności Konsultacja z organem nadzorczym konieczna w momencie kiedy Administrator nie jest w stanie zredukować ryzyka do poziomu przynajmniej średniego mimo, że przewidział wprowadzenie środków bezpieczeństwa

§9
Ocena ryzyka dla przetwarzania danych osobowych

1. Ocena ryzyka składa się z następujących elementów;
1/. Określenie grupy czynności przetwarzania, dla której zostało zidentyfikowane ryzyko,
2/. Aktyw, dla którego zostało zidentyfikowane ryzyko,
3/. Kategoria zagrożenia,
4/. Rodzaj zagrożenia,
5/. Atrybut, dla którego zidentyfikowano ryzyko,
6/. Poziom ryzyka przed wprowadzeniem działań naprawczych wraz ze skalą ryzyka po wstępnym procesie,
7/. Szacowanie ryzyka,
8/. Podjęta przez Administratora decyzja wobec zidentyfikowanego ryzyka,
9/. Zalecenia wobec zidentyfikowanego ryzyka.
2. Administrator może podjąć cztery rodzaje decyzji wobec zidentyfikowanego ryzyka;
1/. Redukcja ryzyka (modyfikacja ryzyka) – polega na obniżeniu poziomu ryzyka poprzez np. zastosowanie dodatkowych zabezpieczeń,
2/. Akceptacja ryzyka (zachowanie ryzyka) – nadleśnictwo nie wprowadza żadnych zmian w zakresie zidentyfikowanego ryzyka (najczęściej do przyjęcia na poziomie

niskim),

3/. Unikanie ryzyka – polega na unikaniu przez nadleśnictwo działań determinujących powstanie określonych typów ryzyka,

4/. Dzielenie (transfer) ryzyka – polega na przeniesieniu ryzyka najczęściej poprzez scedowanie skutków ryzyka na podmiot zewnętrzny.

§10

Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń

1. Plan postępowania z ryzykiem określa;

1/. Określenie grupy czynności przetwarzania, dla której zostało zidentyfikowane ryzyko,

2/. Aktyw, dla którego zostało zidentyfikowane ryzyko,

3/. Kategoria zagrożenia,

4/. Rodzaj zagrożenia,

5/. Atrybut, dla którego zidentyfikowano ryzyko,

6/. Zalecenia wobec zidentyfikowanego ryzyka,

7/. Komórkę organizacyjną odpowiedzialną za wprowadzenie zaleceń,

8/. Termin realizacji wdrożenia zaleceń,

9/. Poziom ryzyka po wprowadzeniu działań naprawczych (wtórny proces szacowania ryzyka) wraz ze skalą ryzyka po wprowadzeniu działań,

10/. Właściciela ryzyka.

§11

Akceptacja ryzyka szczątkowego

Akceptacja ryzyka przez Administratora następuje w oparciu przeprowadzoną analizę ryzyka.

§12

Konsultacje z organem nadzorczym

Jeżeli pomimo zastosowania odpowiednich środków technicznych lub organizacyjnych, analiza następstw utraty poufności bądź integralności lub dostępności w kontekście czynności przetwarzania sklasyfikowanych do Oceny Skutków dla Przetwarzania Danych (DPIA) w dalszym ciągu powoduje wysokie ryzyko szczątkowe, Administrator konsultuje się z organem nadzorczym. Administrator ma świadomość, iż ryzyko wysokie nie może podlegać decyzji w formie akceptacji.

§13
Monitorowanie i przegląd ryzyka

1. Administrator deklaruje chęć utrzymania założonego poziomu bezpieczeństwa danych osobowych przetwarzanych w nadleśnictwie poprzez;

1/. Przeprowadzanie przeglądów ryzyka,

2/. Przeprowadzanie stanu bezpieczeństwa,

3/. Przeprowadzanie oceny skutków względem już poddanych przeglądowi w zakresie praw i wolności czynności przetwarzania, nie rzadziej, niż raz na 3 lata,

4/. Przeprowadzanie oceny skutków dla nowych kategorii przetwarzania czy zastosowania nowoczesnych technologii przetwarzania, przed rozpoczęciem ich przetwarzania z uwzględnieniem ochrony danych w fazie projektowania oraz domyślnej ochrony danych,

5/. Stosowanie procedur postępowania w przypadku wystąpienia incydentu,

6/. Przeprowadzanie szkoleń z zakresu ochrony danych osobowych,

7/. Ustalenie odpowiedzialności za ciągły proces minimalizacji ryzyka.

2. Administrator uwzględnia fakt, iż prowadzenie Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania Danych (DPIA) jest procesem ciągłym, a nie jednorazowym.

NADLEŚNICZY
Nadleśnictwo
Opole
Marek Cholewa
01.02.2021 r.