Załącznik A

Polityka Ochrony Danych Osobowych w Biebrzańskim Parku Narodowym z siedzibą w Osowcu-Twierdzy

SPIS TREŚCI

1 WSTĘP

Administrator, traktując informacje jako newralgiczny zasób każdej organizacji, świadomy zagrożeń wynikających z postępującego rozwoju technologii przetwarzania danych osobowych wprowadza niniejszą Politykę Ochrony Danych.

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (także jako RODO) oraz Ustawy o ochronie danych osobowych.

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie zgodnie z zasadą rozliczalności, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem. Celem Polityki jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania danych osobowych. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz osoby upoważnione do przetwarzania danych osobowych w imieniu Administratora. Celem Polityki jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby zapewnić właściwą ochronę danych osobowych, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem

Opisane i zastosowane w niej zabezpieczenia mają zapewnić:

1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane osobom nieupoważnionym,
2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały w sposób nieautoryzowany zmienione lub zniszczone.
3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny wyłącznie tej osobie,
4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.

Każda osoba posiadająca dostęp do danych osobowych przetwarzanych przez Administratora jak i przetwarzająca dane osobowe z upoważnienia Administratora lub podmiotu przetwarzającego, jest zobowiązana do zapoznania się i stosowania niniejszej Polityki Ochrony Danych Osobowych.

DEFINICJE

Administrator (dalej także jako 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. Administratorem danych osobowych jest Biebrzański Park Narodowy z siedzibą w Osowcu Twierdzy, Osowiec-Twierdza.

Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.

Analiza ryzyka - etap w zarządzaniu ryzykiem polegający na określeniu prawdopodobieństwa wystąpienia zagrożenia, w celu określenia wartości punktowej ryzyka.

Anonimizacja - zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.

Inspektor Ochrony Danych (dalej także jako IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Integralność - zapewnienie, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

Naruszenie (ochrony danych osobowych) - jest to przypadkowy lub niezgodny z prawem incydent, prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem Inspektora Ochrony Danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Podatność - słabość, luka lub brak odpowiednich zabezpieczeń w systemie, które mogą umożliwić zaistnienie zagrożenia.

Podmiot przetwarzający (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Profilowanie – jest dowolną 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.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych. Obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).

Rozliczalność - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą

również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Zagrożenie - potencjalne naruszenie (potencjalny incydent).

2 OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator / Podmiot przetwarzający nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

2.1 OPIS OPERACJI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane **w załączniku nr 1. Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).**
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
    1) nazwę zbioru (opis kategorii osób),
    2) opis celów przetwarzania,
    3) charakter, zakres, kontekst danych osobowych,
    4) odbiorcy danych,
    5) funkcjonalny opis operacji przetwarzania,
    6) aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing),
    7) informacja o konieczności wpisu do rejestru czynności przetwarzania,
    8) informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

2.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO).

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator/ Podmiot przetwarzający zobowiązany jest do spełnienia obowiązków prawnych wobec danych w zbiorach (dla kategorii osób) znajdujących się w **załączniku - nr 1. Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).**

W szczególności należy zapewnić, że :

1) dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
2) dane te są adekwatne w stosunku do celów przetwarzania,
3) dane te są przetwarzane przez określony czas (retencja danych),
4) wobec osób których dane są przetwarzane wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
5) opracowano informacje dotyczące przetwarzania danych osobowych dla poszczególnych osób. Informacje dostępne są w poszczególnych działach i udostępniane przez pracowników działów osobom których dane dotyczą. Informacje dotyczące przetwarzania danych osobowych są udostępniane także na stronie internetowej Biebrzańskiego Parku Narodowego oraz Biuletynie Informacji Publicznej,
6) zostały zwarte umowy powierzenia z podmiotami przetwarzającymi zgodnie z art. 28 RODO. Wykaz podmiotów przetwarzających prowadzony jest w **załączniku nr 2. Rejestr umów powierzenia.**

2.3 ANALIZA RYZYKA.

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów).

2.3.1 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.

2.3.2 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną Skalę skutków prezentuje Tabela B.
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P* S.**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

2.3.3 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Proponowaną skalę Ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	**WARTOŚĆ** [**R = P*S**]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

2.3.4 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    1) przeniesienie – przerzucenie ryzyka na inną organizację *(np. outsourcing, ubezpieczenie),*
    2) unikanie – eliminacja działań powodujących ryzyko *(np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji),*
    3) redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (*np. zaszyfrowanie komputerów przenośnych oraz pendrivów z danymi wynoszonych poza organizację),*
3. Analizę ryzyka przeprowadza się w specjalnym szablonie (programie) lub w wersji papierowej stanowiącej **załącznik nr 3 - Arkusz analizy ryzyka RODO.**

2.3.5 Ponowna analiza ryzyka.

Ponowna analiza ryzyka przeprowadzana jest cyklicznie nie rzadziej niż raz na 2 lata lub po znaczących zmianach w przetwarzaniu danych *(np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).*

2.4 PLAN POSTĘPOWANIA Z RYZYKIEM.

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

3 UPOWAŻNIENIA.

1. Administrator lub podmiot przetwarzający jeśli działa na polecenie Administratora odpowiada za nadawanie lub cofanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.
2. Każda osoba upoważniona może przetwarzać dane wyłącznie na wyraźne polecenie Administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są na wniosek przełożonych osób, którym nadawane ma zostać upoważnienie. Upoważnienia określają zakres operacji na danych do których upoważnia się poszczególne osoby.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia.
5. Wzór upoważnienia stanowi **załącznik nr 4 – upoważnienie do przetwarzania danych osobowych.**
6. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy w celu wypełnienia zasady rozliczalności i adekwatności określonej przepisami RODO i stanowi **załącznik nr 5 – ewidencja osób upoważnionych do przetwarzania danych osobowych.**
7. Osoby upoważnione do przetwarzania danych osobowych odpowiedzialne są za:
    1) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa Danych Osobowych, Regulaminu Ochrony Danych Osobowych i Instrukcji Zarządzania Systemami Informatycznymi,
    2) stosowanie się do zaleceń Administratora w zakresie ich kompetencji,
    3) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez Administratora w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych,

4) niezwłoczne informowanie Administratora lub Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w Biebrzańskim Parku Narodowym o których pracownik posiada wiedzę,
5) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
6) korzystanie z systemów informatycznych Biebrzańskiego Parku Narodowego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych oraz przyjętych procedur dla danego stanowiska,
7) zachowanie w tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji,
8) dokonywanie wszelkich operacji wykonywanych w systemach informatycznych przy użyciu przydzielonego identyfikatora oraz hasła,
9) zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

4 ŚRODKI ORGANIZACYJNE I TECHNICZNE ZABEZPIECZAJĄCE DANE OSOBOWE

Administrator jest zobowiązany do stosowania środków technicznych i organizacyjnych (zabezpieczeń) adekwatnych do zagrożeń naruszenia praw i wolności osób.

1. Administrator prowadzi uproszczony wykaz stosowanych zabezpieczeń w postaci **załącznika nr 6 - Wykaz zabezpieczeń RODO**.
2. Zabezpieczenia są opisane także w formie przyjętych procedur.
3. Wykaz zabezpieczeń powinien być aktualizowany, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka / oceny skutków.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe w zakresie bezpiecznych zasad przetwarzania. Regulamin stanowi **załącznik nr 7.**

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

6 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator.
3. Szkolenia (stanowiskowe lub poszczególnych działów) związane z ochroną danych osobowych może wykonywać Inspektor Ochrony Danych.

4. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych dokumentuje się odbycie tego szkolenia w postaci listy uczestników z ich podpisami.
5. Materiały szkoleniowe dla uczestników szkolenia będą dostępne w taki sposób, aby każda osoba uczestnicząca w szkoleniu mogła się z nimi zapoznać także po zakończeniu szkolenia. W każdym czasie, pracownicy mogą zwracać się do Inspektora Ochrony Danych o instrukcje lub wyjaśnienia w zakresie ochrony danych osobowych.
6. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, w formie oświadczenia.
7. Nowi pracownicy i współpracownicy muszą obowiązkowo przejść szkolenie z zakresu ochrony danych osobowych przed ich dopuszczeniem do wykonywania obowiązków służbowych, co powinno zostać udokumentowane stosownym oświadczeniem.

7 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
4. W przypadku stwierdzenia wystąpienia incydentu, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
    1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
    2) inicjuje ewentualne działania dyscyplinarne,
    3) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
    4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia,

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w rejestrze incydentów stanowiącym **załącznik nr 8.**
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych, pod sankcją kar dyscyplinarnych wynikających z prawa pracy oraz obowiązku naprawienia ewentualnej szkody.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Administrator zgłasza je organowi nadzorczemu.
8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
9. W sprawach związanych z incydentami/naruszeniami ochrony danych osobowych bierze udział także Inspektor Ochrony Danych, który powinien zostać powiadomiony o wystąpieniu incydentu/naruszenia niezwłocznie po jego ujawnieniu.

8 REJESTR CZYNNOŚCI PRZETWARZANIA

1. Administrator prowadzi rejestr zgodnie z **załącznikiem nr 1. Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).**
2. Jako podmiot przetwarzający Biebrzański Park Narodowy prowadzi rejestr zgodnie z **załącznikiem nr 1A. - Rejestr kategorii czynności przetwarzania.**

9 AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W tym celu Administrator stosuje procedurę audytów – **załącznik nr 9.**

10 PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO (BCP)

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w **załączniku nr 10 Plan ciągłości działania.**

11 SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH.

1. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane są przetwarzane.
2. Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym zamieszczanie na stronie internetowej (Biuletynie Informacji Publicznej) informacji lub odwołań (linków) do informacji o prawach osób, sposobie korzystania, identyfikacji.

3. W celu realizacji praw osób, Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzić do nich zmiany i usunąć w sposób zintegrowany.
4. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób. Przykładowy Rejestr obsługi stanowi **Załącznik nr 11**
5. Realizując prawa osób których dane dotyczą, Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przenoszenia danych może niekorzystnie wpłynąć na prawa i wolności osób trzecich, Administrator może zwrócić się do osoby celem wyjaśnienia wątpliwości lub podjąć inne prawnie przewidziane środki, łącznie z odmową zadośćuczynienia żądaniu.
6. Administrator informuje osobę o tym, że nie przetwarza jej danych jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
7. Administrator informuje osobę w terminie miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i prawach osoby z tym związanych.
8. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę czy przetwarza jej dane oraz informuje o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z tym zastrzeżeniem, że kopii danych wydanych przy realizacji prawa dostępu do danych Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
9. Na żądanie osoby Administrator wydaje kopie danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Za wydanie kolejnej kopii danych mogą zostać pobrane opłaty skalkulowane na podstawie oszacowanego jednostkowego koszu obsługi żądania wydania kopii danych.
10. Administrator dokonuje sprostowania danych na żądanie osoby, której dane dotyczą.
11. Administrator dokonuje uzupełnienia danych na żądanie osoby, której dane dotyczą.
12. Na żądanie osoby której dane dotyczą Administrator usuwa dane gdy:
    1) dane nie są niezbędne do celów w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
    2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy ich przetwarzania,
    3) osoba której dane dotyczą wniosła skuteczny sprzeciw przeciwko przetwarzaniu tych danych,
    4) dane były przetwarzane niezgodnie z prawem,
    5) konieczność usunięcia wynika z obowiązku prawnego.
13. Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki określone w art. 17 ust. 3 RODO.
14. Administrator dokonuje ograniczenia przetwarzania na żądanie osoby gdy:
    1) osoba kwestionuje prawidłowość danych - na okres pozwalający sprawdzić ich prawidłowość,
    2) przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystania,
    3) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie której dane dotyczą do ustalenia, dochodzenia lub obrony przysługujących jej roszczeń,

4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstawy sprzeciwu.

15. W razie wątpliwości dotyczących obsługi obowiązków informacyjnych, zawiadomień i żądań osób, których dane dotyczą lub powziętych w innych sprawach związanych z ochroną danych osobowych, zasadne jest skorzystanie z opinii/porady Inspektora Ochrony Danych.

Na żądanie osoby, której dane dotyczą Administrator wydaje w ustrukturyzowanym powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli to możliwe, dane dotyczące osoby, która dostarczyła Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Administratora.

12 MONITORING WIZYJNY.

Administrator prowadzi monitoring wizyjny obiektów w celu zapewnienia bezpieczeństwa pracowników oraz ochrony mienia znajdującego się na terenie Biebrzańskiego Parku Narodowego.

Regulamin monitoringu wizyjnego stanowi **załącznik nr 12.**

13 UWZGLĘDNIANIE OCHRONY DANYCH OSOBOWYCH NA ETAPIE PROJEKTOWANIA NOWYCH ROZWIĄZAŃ.

Administrator, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, w celu skutecznej realizacji opisanych wyżej zasad oraz spełnienia wymagań, wdraża odpowiednie środki techniczne i organizacyjne zaprojektowane w celu ochrony danych.

Wszelkie nowe operacje, procesy lub transakcje, przed ich wdrożeniem muszą zostać poddane udokumentowanej ocenie z punktu widzenia ochrony danych osobowych, tak by zapewnić identyfikację wszystkich odpowiednich środków technicznych i organizacyjnych ochrony danych osobowych, a następnie konsekwentnego ich stosowania w trakcie realizacji operacji, procesu lub transakcji (tzw. również **Privacy by design**). Należy przy tym jeśli to konieczne skonsultować nowe operacje, procesy, transakcje przed ich wdrożeniem z Inspektorem Ochrony Danych wyznaczonym u Administratora.

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (tzw. również **Privacy by default**). Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności powyższe działania muszą zostać podjęte w trakcie projektowania, rozwijania, wyboru lub używania oprogramowania, usług lub towarów, które mają wpływ na przetwarzanie danych osobowych lub pozostają w związku z danymi osobowymi. Należy przy tym jeśli to konieczne skonsultować nowe środki techniczne i organizacyjne przed ich wdrożeniem z Inspektorem Ochrony Danych wyznaczonym u Administratora.

Aby wykonać powyższe zadania, należy zapewnić, że IOD został we właściwym czasie i we właściwy sposób zaangażowany we wszystkie operacje, czynności i transakcje związane z ochroną danych

osobowych. Zapewnienie już na wstępie, że IOD zostanie poinformowany oraz zostanie zasięgnięta jego opinia, ułatwi przestrzeganie obowiązujących przepisów i zapewni ochronę prywatności z uwzględnieniem zasady „privacy by design", powinno to być zatem standardową procedurą w Biebrzańskim Parku Narodowym.

14 PODSTAWOWE WYMAGANIA W STOSUNKU DO PODMIOTU PRZETWARZAJĄCEGO.

1. Podstawowe Wymagania w stosunku do Przetwarzającego

Ilekroć w odniesieniu do konkretnego Przetwarzania Danych Osobowych Biebrzański Park Narodowy wyznacza podmiot przetwarzający dane osobowe, zobowiązany on jest:

1) przetwarzać dane osobowe zgodnie z zasadami określonymi w niniejszej Polityce oraz obowiązującymi przepisami i regulacjami dotyczącymi ochrony danych osobowych;
2) dopilnować, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub były zobowiązane do zachowania poufności;
3) przetwarzać dane osobowe zgodnie z instrukcjami Administratora, chyba że obowiązujące przepisy stanowią inaczej;
4) prowadzić rejestr wszystkich czynności związanych z przetwarzaniem danych;
5) wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony Przetwarzania danych;
6) w razie potrzeby wyznaczyć Inspektora Ochrony Danych;
7) podpisać umowę lub inny akt prawny regulujący stosunki z Administratorem;
8) powstrzymać się od wyznaczenia dalszego podmiotu przetwarzającego dane bez uprzedniej wyraźnej zgody Administratora. Jeśli Przetwarzający otrzymał ogólne pisemne upoważnienie do dalszego powierzania czynności Przetwarzania danych, zobowiązany jest w odpowiednim czasie poinformować Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających dane w celu umożliwienia Administratorowi zgłoszenia sprzeciwu wobec takich zmian;
9) Przetwarzający powierzając Przetwarzanie danych dalszym podmiotom w celu przeprowadzenia określonych czynności przetwarzania w imieniu Administratora zobowiązany jest zawrzeć umowę z tym dalszym Przetwarzającym, aby nałożyć na niego takie same obowiązki w zakresie ochrony danych osobowych, jak określone w umowie powierzenia przetwarzania danych osobowych łączącej go z Administratorem;
10) udzielać pomocy Administratorowi w wypełnianiu jego obowiązków związanych z realizacją wniosków w zakresie praw osób, których dane dotyczą.

Administrator przed wyborem danego podmiotu przetwarzającego (procesora) zobowiązany jest odebrać od tego podmiotu ankietę „Kryteria doboru procesora" – stanowiącej **załącznik nr 13 do Polityki** oraz dokonać jej szczegółowej analizy w celu weryfikacji danego podmiotu pod kątem wymagań formalnych związanych z przetwarzaniem danych osobowych oraz móc udokumentować swoje działania zgodnie z zasadą rozliczalności.