Zarządzenie Nr 28
Nadleśniczego Nadleśnictwa Świdwin
z dnia 15 czerwca 2020r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Nadleśnictwie Świdwin
NN.0171.2.2020.CK

Na podstawie § 22 ust. 3 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe stanowiące załącznik do Zarządzenia nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. w sprawie nadania statutu Państwowemu Gospodarstwu Leśnemu Lasy Państwowe oraz na podstawie art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/67 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016),

zarządzam, co następuje:

§ 1. Wprowadzam w życie "Politykę Ochrony Danych Osobowych w Nadleśnictwie Świdwin" stanowiącą załącznik nr 1 do niniejszego zarządzenia.
§ 2. Zobowiązuję wszystkich pracowników Nadleśnictwa Świdwin do przestrzegania dokumentacji "Polityki Ochrony Danych Osobowych w Nadleśnictwie Świdwin".
§ 3. Zarządzenie wchodzi w życie z dniem 1 lipca 2020 roku.

NADLEŚNICZY
Rafał Grzegorczyk

Załączniki:
1. Polityka Ochrony Danych Osobowych w Nadleśnictwie Świdwin.

Załącznik nr 1 do Zarządzenia nr 28
Nadleśniczego Nadleśnictwa Świdwin
z dnia 15 czerwca 2020r.

Polityka ochrony danych osobowych w Nadleśnictwie Świdwin

§1.

1. Słowniczek:

   Dane osobowe – wszelkie 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 operację 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.

2. Niniejszy dokument określa środki techniczne i organizacyjne zastosowane w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Nadleśnictwie Świdwin zwanym dalej Nadleśnictwem.
3. Celem niniejszej Polityki ochrony danych osobowych (PODO) jest wypełnienie założeń Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej też zwane RODO) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018.1000 z późn. zm.)
4. Opisane reguły określają granice dopuszczalnego zachowania wszystkich osób upoważnionych do przetwarzania danych osobowych w nadleśnictwie.
5. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby nie przestrzegające zapisów polityki i prawa w zakresie ochrony danych osobowych.
6. PODO określa procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń w tym prowadzenia wymaganych rejestrów czynności

przetwarzania oraz zasad postępowania w przypadku naruszeń ochrony danych i zgłaszania naruszeń wraz z prowadzeniem odpowiednich rejestrów.

7. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz szkolenia pracowników, pozwalają zgodnie z prawem wypełnić obowiązki w zakresie ochrony danych osobowych.
8. PODO określa tryb postępowania dotyczący:
   - prowadzenie rejestrów czynności przetwarzania, o których mowa w art. 30 RODO;
   - zgłaszanie naruszenie ochrony danych do organu nadzorczego – art. 33 ust 3 RODO;
   - prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO;
   - zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7,
   - wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z obowiązującym prawem;
9. PODO obowiązuje wszystkie osoby upoważnione do przetwarzania danych osobowych w nadleśnictwie.

§ 2.

1. Miejsca, w których przetwarzane są dane osobowe to:
   1) budynek biura nadleśnictwa,
   2) kancelarie leśniczówek.
2. We wszystkich w/w budynkach/pomieszczeniach znajdują się szafy wykonane z płyt wiórowych, zamykane na zamki patentowe.
3. Biuro nadleśnictwa i kancelarie czynne są w godzinach 7.00-15.00.
4. Po godzinach pracy biura nadleśnictwa, do pomieszczeń posiadają dostęp: nadleśniczy, zastępca nadleśniczego, główny księgowy, sekretarz, inżynier nadzoru, sekretarka, dyżurny Punktu Alarmowo – Dyspozycyjnego, komendant straży leśnej oraz osoba sprzątająca, natomiast do pomieszczeń kancelarii w leśnictwach dostęp mają wyłącznie leśniczowie i podleśniczowie.

§ 3.

5. Budynek biura nadleśnictwa z zewnątrz i wewnątrz wyłącznie w celu zapewnienia bezpieczeństwa jest wyposażony w detektory ruchu połączone z zewnętrzną firmą monitorującą.
6. Na drzwiach wejściowych do budynku umieszcza się tabliczkę informacyjną o stosowaniu detektorów ruchu.
7. Na tablicy informacyjnej znajdującej się wewnątrz budynku umieszcza się informację o stosowaniu detektorów ruchu w celu wypełnienia obowiązku informacyjnego wynikającego z art. 13 RODO. Treść informacji stanowi załącznik

nr 1.

8. Budynek gospodarczy szkółki leśnej Kartlewo jest monitorowany z zewnątrz wyłącznie w celu zapewnienia bezpieczeństwa.
9. Przetwarzanie zapisu z monitoringu nie narusza praw i wolności osoby, której dane dotyczą.
10. Obraz z kamer wyświetlany jest na monitorze i dodatkowo rejestrowany na dysku twardym o pojemności 2 TB zlokalizowanym na terenie w/w obiektu w kancelarii leśniczego szkółkarza Do pomieszczenia i zgromadzonych danych ma wyłącznie osoba upoważniona przez Nadleśniczego.
11. Przetwarzanie danych z zapisu monitoringu jest możliwe po zalogowaniu się do systemu za pomocą nadanego loginu i hasła. Login i hasło nadaje Administrator sieci zgodnie z Polityką SILP, przyjmując zasady jak przy nadawaniu uprawnień do SILP.
12. Pomieszczenie kancelarii leśniczego szkółkarza jest zamykane na drzwi przeciwpożarowe antywłamaniowe wyposażone w atestowane zamki.
13. Obraz z kamer jest zachowywany jest w systemie tzw. pętli na okres 3 miesięcy. System obserwacji z kamer jest w pełni zautomatyzowany, nie wymaga nadzoru oraz obsługi, sygnał nie jest przesyłany poza obiekt.
14. Udostępniane danych będzie się odbywało wyłącznie na zasadach określonych w przepisach szczególnych.
15. Na drzwiach wejściowych do budynku umieszcza się tabliczkę informacyjną o stosowaniu monitoringu.
16. Na tablicy informacyjnej znajdującej się wewnątrz budynku umieszcza się informację o monitoringu w celu wypełnienia obowiązku informacyjnego wynikającego z art. 13 RODO. Treść informacji stanowi załącznik nr 1.
17. Dla danych osobowych które są powierzane do przetwarzania należy zawrzeć umowę powierzenia, zgodnie z wymogami RODO określonymi w art. 28. Rejestr umów powierzenia przetwarzania danych prowadzi inżynier nadzoru Cezary Kłoczko, wzór rejestru stanowi załącznik nr 2a.

§ 4.

Dla potrzeb ochrony danych osobowych przetwarzanych w formie papierowej stosuje się zabezpieczenia polegające na przechowywaniu:

- dokumentacji bieżącej – w szafach zamykanych na zamki w obszarach przetwarzania danych osobowych,
- dokumentacji archiwalnej - w składnicy akt;
- dokumentacji pracowniczej – w pokoju nr 5 (stanowisko ds. pracowniczych).

§ 5.

1. Wprowadza się następujące zabezpieczenia danych:

1.1. Przetwarzanych na urządzeniach elektronicznych:

1.1.1. Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom kontroli konta użytkownika, umożliwiający wykonywanie operacji mających wpływ na stabilność działania systemu wyłącznie przez użytkowników z uprawnieniami administratora systemu.

1.1.2. Uprawnienia administratora systemu posiadają wyłącznie pracownicy, którym powierzono wykonywanie obowiązków administratora.

1.1.3. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.

1.1.4. Zalogowanie się do systemu, wymaga podania kodu PIN do karty kryptograficznej bądź nazwy użytkownika i hasła.

1.1.5. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji. Nieudane próby logowania są rejestrowane, a po 3 nieudanych próbach logowania następuje czasowa blokada konta. Odblokowania konta może dokonać tylko właściwy administrator systemu. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.

1.1.6. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się systemy „zapór ogniowych" zabezpieczających sieć lokalną oraz systemy operacyjne stacji roboczych.

1.1.7. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe. Aktualizacja bazy wirusów wykonywana jest automatycznie, kilka razy w ciągu doby. Za prawidłowość funkcjonowania systemu antywirusowego odpowiada administrator sieci.

1.1.8. W pokoju, do którego dostęp mają petenci, monitory komputerowe ustawione
są w sposób uniemożliwiający odczyt z ekranu przez klientów/petentów.

1.1.9. Po zakończeniu dnia pracy należy wyłączyć komputer i wszelkie urządzenia elektroniczne.

1.1.10. Kopie bezpieczeństwa ze stacji roboczych wykonywane są automatycznie
w zdalny zasób.

1.1.11. Pracownik opuszczając stanowisko pracy/pokój w ciągu dnia roboczego jest zobowiązany do zablokowania komputera (stacji roboczej).

1.2. Przetwarzanych w formie papierowej:

1.2.1. Kartoteki papierowe znajdują się w meblowych szafach, zamykanych na zamki meblowe w pokojach, w których przetwarzane są dane osobowe.

1.2.2. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.

1.2.3. Pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu niezbędne do pracy w danym momencie. Należy

unikać przechowywania dokumentów niepotrzebnych do bieżących zadań.

1.2.4. Na biurku nie powinny znajdować się napoje i żywność w pojemnikach grożących rozlaniem.

1.2.5. Po zakończeniu pracy z dokumentami zawierającymi dane osobowe należy odłożyć je do szuflady lub szafy zamykanej na klucz.

1.2.6. Dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji należy niszczyć w niszczarce spełniającej normę DIN 66399 (klasa nie niższa niż P3).

1.3. Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:

1.3.1. Dostęp do danych mają wyłącznie pracownicy upoważnieni przez Nadleśnictwo. Rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych, łącznie z ich identyfikatorami w systemie prowadzony jest przez Administratora danych.

1.3.2. W przypadku gdy pracownik sam zajmuje pokój, przed jego opuszczeniem jest zobowiązany zamknąć drzwi wejściowe do pokoju na klucz.

1.3.3. W przypadku gdy w pokoju znajduje się kilka stanowisk roboczych, pracownik opuszczający pokój jako ostatni jest zobowiązany zamknąć drzwi wejściowe do pokoju na klucz.

1.3.4. Po zakończeniu pracy na biurku nie powinny pozostać jakiekolwiek dokumenty zawierające dane osobowe.

§ 6.

Procedury nadawania upoważnień do przetwarzania danych osobowych

1. Pracownicy przetwarzający dane osobowe przed przystąpieniem do ich przetwarzania, zobowiązani są do zapoznania się z aktualnymi przepisami prawa dot. ochrony danych osobowych i PODO.
2. Upoważnienie do przetwarzania danych stanowi załącznik nr 3
3. Nadanie odpowiednich uprawnień w Systemie Informatycznym Lasów Państwowych (dalej „SILP") następuję zgodnie z POLITYKĄ SILP i następuje po otrzymaniu upoważnienia o którym mowa w pkt 2. § 11. Pracownicy są zobowiązani do pracy w SILP zgodnie z jej zapisami, zgodnie z zał. nr 10.
4. Rejestr upoważnień do przetwarzania danych osobowych prowadzi inżynier nadzoru Cezary Kłoczko, zgodnie ze wzorem zał. nr 4.

§ 7.

Zasady udostępniania danych

Dane są udostępniane wyłącznie na zasadach określonych w obowiązujących przepisach

o ochronie danych osobowych lub innych aktach prawnych, w tym przepisach szczególnych umożliwiających udostępnianie tych danych.

§ 8.

Kontrola przestrzegania zasad bezpieczeństwa

1. Osoba wyznaczona przez Nadleśniczego sprawuje nadzór nad przestrzeganiem PODO i przetwarzania danych osobowych w nadleśnictwie.
2. Osoba ta może dokonywać okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad i procedur bezpieczeństwa.
3. Okresowe kontrole przestrzegania zasad powinny odbywać się przynajmniej raz
   w roku.
4. Osoba odpowiedzialna za przeprowadzenie kontroli zobowiązana jest do sporządzania protokołów z kontroli.
5. Raport z kontroli przekazywany jest Nadleśniczemu.
6. Przedmiotem kontroli w szczególności powinny być:
   - zgodność procesów z wymaganiami prawnymi w zakresie przetwarzania danych osobowych,
   - funkcjonowanie systemów informatycznych i zabezpieczeń fizycznych,
   - poprawność funkcjonowania aplikacji przetwarzających dane osobowe,
   - zgodność wydanych upoważnień ze stanem faktycznym osób przetwarzających dane,
   - nadanie uprawnień użytkownikowi SILP zgodnie z upoważnieniem,
   - zasady i sposoby niszczenia dokumentów i nośników elektronicznych,
   - zasady przestrzegania zabezpieczenia pomieszczeń i systemów informatycznych, podczas nieobecności pracownika,
   - zasady przechowywania dokumentów zawierających dane osobowe,
   - zasad przestrzegania obowiązków informacyjnych,
   - zasad zbierania danych.
7. Kontroli wykorzystania systemu informatycznego dokonuje Administrator sieci.
8. Przynajmniej raz w roku Administrator sieci wykonuje weryfikację zainstalowanego oprogramowania.

§ 9.

Odpowiedzialność osób upoważnionych do przetwarzania danych

1. Zasady i procedury zawarte w PODO obowiązują wszystkich pracowników nadleśnictwa.
2. Każdy pracownik jest indywidualnie odpowiedzialny za prawidłowe i zgodne z prawem przetwarzanie danych.
3. Każdy pracownik jest indywidualnie odpowiedzialny za przetwarzane przez

siebie informacji w formie tradycyjnej (papierowej) jak i w formie elektronicznej.

4. Za umożliwienie korzystania z urządzeń elektronicznych przez osobę nieupoważnioną odpowiada pracownik, któremu sprzęt ten został przydzielony.
5. Na każdym pracowniku upoważnionym do przetwarzania danych spoczywa odpowiedzialność za rodzaj i zakres danych przetwarzanych przez niego w ramach przydzielonych mu uprawnień, oraz odpowiedzialność za ochronę tych danych przed niepowołanym dostępem, niepowołaną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.

§ 10

Zbieranie danych osobowych zgodnie z art. 5 RODO

1. Należy zbierać dane wyłącznie niezbędne do wykonania obowiązków wynikających
   z przepisów prawa, sprawowania władzy publicznej lub realizacji celów w jakim są pozyskiwane.
2. Dane osobowe muszą być:

2.1. Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

2.2. Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

2.3. Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

2.4. Prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;.

2.5. Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

2.6. Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

3. Pracownik przetwarzający dane osobowe jest odpowiedzialny za przestrzeganie zasad określonych w ust. 1 i 2, i musi być w stanie wykazać ich przestrzeganie.
4. W przypadku gdy nadleśnictwo nie jest administratorem który zbiera dane, a jedynie je otrzyma od administratorów zewnętrznych, to należy je przetwarzać wyłącznie
   w celu, w jakim zostały zebrane i stosować zasady postępowania i zabezpieczenia jak określono w niniejszym dokumencie np. dane otrzymane w

ramach porozumień, realizacji umów, realizacji wspólnych przedsięwzięć, itp.

§ 11.

Obowiązek informacyjny zgodnie z art. 12 ust. 1 RODO

1. Każdy pracownik podczas pozyskiwania danych osobowych w ramach wykonywania obowiązków służbowych:
   - od osoby, której dane dotyczą;
   - w sposób inny niż od osoby, której dane dotyczą;
   - przez cały okres przetwarzania danych osobowych (w związku z prawem dostępu przysługującym osobie, której dane dotyczą);

jest zobowiązany wypełnić obowiązek informacyjny wynikający z art. 12 ust. 1 RODO.

2. Sposoby udzielania informacji i ich odbiorcy:
   2.1. Na piśmie:
   a) Pracownicy Nadleśnictwa – zgodnie ze wzorem w zał. nr 5. Klauzula informacyjna powinna być podpisana przez pracownika i opatrzona datą potwierdzającą zapoznanie się z jej treścią.
   b) Klienci – zgodnie ze wzorem zał. nr 6.

   Klauzulę informacyjną należy zamieścić w:
   - wszelkich formularzach (np. podania, wnioski, prośby, kwestionariusze, zezwolenia, itp.) dostarczanych przez Nadleśnictwo,
   - fakturach,

   w których znajdują się dane osobowe.

   c) Petenci – zgodnie ze wzorem w zał. nr 6.

   Klauzulę informacyjną należy zamieścić w:
   - wszelkich formularzach (np. podania, wnioski, prośby, kwestionariusze, itp.) dostarczanych przez Nadleśnictwo w których znajdują się dane osobowe;
   - dokumentach wystawianych przez Nadleśnictwo w których znajdują się dane osobowe.

   d) Strony umowy (np. najmu, dzierżawy, użyczenia, udostępnienia, dostawy, usługi, itd.) zgodnie z zał. nr 6.

   Klauzula informacyjna powinna być podpisana przez stronę umowy i opatrzona datą potwierdzającą zapoznanie się z jej treścią. Nie należy umieszczać klauzuli informacyjnej w treści umowy.

   Klauzula informacyjna w zależności od możliwości technicznych jej dodania do

dokumentu może stanowić:

- odrębny dokument,
- dokument opatrzony pieczęcią zawierającą treść klauzuli,
- stopkę dokumentu.

2.2. Elektronicznie – zgodnie z zał. nr 6. Stosuje się wyłącznie w przypadku gdy komunikacja z osobą fizyczną odbywa się wyłącznie drogą elektroniczną. Klauzulę należy przesyłać jako załącznik lub stopkę każdorazowo – zgodnie z zał. nr 6a w wiadomościach kierowanych do osoby fizycznej.

2.3. Ustnie – zgodnie za zał. nr 7. Dotyczy wyłącznie danych pozyskiwanych w związku z wypełnianiem zadań z zakresu ochrony lasy przed szkodnictwem leśnym przez Straż Leśną i Służbę Leśną (dotyczy czynów zabronionych).

Jeżeli klient/petent nie skorzysta z formularzy przygotowanych przez Nadleśnictwo, to należy w korespondencji stanowiącej pierwszą odpowiedź w sprawie zawrzeć/załączyć klauzulę informacyjną w sposób jak opisano powyżej.

Wyłącznie w przypadku określonym w pkt 1) lit a) i d) należy na wzorze klauzuli informacyjnej pobrać podpis opatrzony datą potwierdzającą zapoznanie się z jej treścią.

§ 12

Obowiązek prowadzenia rejestrów czynności przetwarzania zgodnie z art. 30 ust. 1 RODO

1. Rejestr należy prowadzić wg. wzoru jak w zał. nr 8 w formie pisemnej, w tym w formie elektronicznej (art. 30 ust. 3 RODO).
2. Wyznacza się obowiązek prowadzenia rejestrów czynności dot. danych osobowych odpowiednio (art. 30 ust. 5 RODO):
    1) pracowników Administratora danych w zakresie kadrowo-płacowym przetwarzanych w związku z zatrudnieniem (przetwarzanie nie ma charakteru sporadycznego);
    2) zgromadzonych w związku z wypełnianiem zadań z zakresu ochrony lasy przed szkodnictwem leśnym przez Straż Leśną i Służbę Leśną (dot. czynów zabronionych przez osoby fizyczne i wyroków skazujących).

Rejestry prowadzą i na bieżąco aktualizują pracownicy wykonujący w/w zadania w

ramach obowiązków służbowych dla których określono obowiązek prowadzenia rejestrów.

§ 13.

Zdarzenia naruszające ochronę danych osobowych

1. Podział zagrożeń:
   - zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
   - zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki, , awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, , może nastąpić naruszenie poufności danych,
   - zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej); zagrożenia te możemy podzielić na: nieuprawniony dostęp do dokumentów w formie papierowej lub do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia danych osobowych to głównie:
   - sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   - niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
   - awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
   - pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   - jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

- naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- próba lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- niedopuszczalna manipulacja danymi osobowymi,
- ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo inne strzeżonych elementów zabezpieczeń,
- praca wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy, wskazująca na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
- podmiana lub zniszczenie nośników/dokumentów z danymi osobowymi bez odpowiedniego upoważnienia; skasowanie lub skopiowanie danych osobowych w sposób niedozwolony,
- rażąco naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości
   w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

§ 14.

Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych określa Instrukcja postępowania w sytuacji naruszenia ochrony danych stanowiąca zał. nr 9.

§ 15.

Postanowienia końcowe

Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego
w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie

z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych,
w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym odpowiednich osób.

Orzeczona kara dyscyplinarna, nie wyklucza odpowiedzialności karnej tej osoby zgodnie z obowiązującym prawem o ochronie danych osobowych oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat, jeżeli takie wystąpią.

NADLEŚNICZY
Rafał Grzegorczyk

Załączniki:

1. Klauzula informacyjna – monitoring.
2. Umowa powierzenia (wzór umowy).

2a. Rejestr umów powierzenia przetwarzania danych.

3. Upoważnienie do przetwarzania danych osobowych.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
5. Klauzula informacyjna (kadry – pracownicy nadleśnictwa).
6. Klauzula informacyjna (ogólna – klienci, petenci).

6a. Stopka maila.

7. Klauzula informacyjna (szkodnictwo leśne).
8. Rejestr czynności przetwarzania.
9. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.
10. Polityka SILP.

Załącznik nr 1

KLAUZULA INFORMACYJNA – MONITORING

Zgodnie z art. 13 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. (zwane dalej RODO) w związku z przetwarzaniem Pana/i danych osobowych uprzejmie informujemy, że:

1. **Budynek biura nadleśnictwa jest** wyłącznie w celu zapewnienia bezpieczeństwa jest wyposażony w detektory ruchu połączone z zewnętrzną firmą monitorującą. Budynek gospodarczy szkółki leśnej Kartlewo jest monitorowany z zewnątrz wyłącznie w celu zapewnienia bezpieczeństwa.
2. **Administratorem Twoich danych osobowych (ADO)** jest: Państwowe Gospodarstwo Leśne Lasy Państwowe Nadleśnictwo Świdwin, ul. Szczecińska 58, 78-300 Świdwin.
3. Nasze dane kontaktowe to: Nadleśnictwo Świdwin, ul. Szczecińska 58, 78-300 Świdwin.
4. W sprawach związanych z danymi osobowymi, jesteśmy dostępni pod adresem e-mail: swidwin@szczecinek.lasy.gov.pl lub pod adresem wskazanym w pkt 3.

5. Cele i podstawy przetwarzania

Przetwarzanie danych osobowych osób fizycznych będących naszymi klientami/petentami odbywa się w celu prawnie uzasadnionego interesu realizowanych przez ADO tj. zapewnienie bezpieczeństwa w obiektach i wokół nich - art. 6 ust. 1 lit. f RODO.

6. Odbiorcy danych

Dane przekazujemy tylko wówczas i tylko w takim zakresie, w jakim jest to rzeczywiście niezbędne i wymagane w myśl bezwzględnie obowiązujących przepisów prawa i w sposób zgodny z tymi przepisami, w tym z przepisami szczególnymi.

7. Dostęp do monitoringu i danych ma wyłącznie osoba upoważniona przez ADO sprawująca nadzór nad bezpieczeństwem przechowywania danych i sprawnością działania systemu.

8. Prawa osób, których dane dotyczą

Informujemy o przysługującym prawie do:

- dostępu do swoich danych osobowych i żądania ich kopii,
- sprostowania (poprawiania) swoich danych,
- żądania ograniczenia przetwarzania swoich danych,
- przenoszenia danych,
- usunięcia danych,
- wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.

9. Informacja o wymogu/dobrowolności podania danych

Podanie danych jest wymagane przepisami prawa.

11. Zautomatyzowane podejmowanie decyzji

Zebrane dane nie będą podlegały automatyzacji podejmowania decyzji oraz nie będą profilowane, a także nie będą przekazywane do państw trzecich.

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 2

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

Skarb Państwa Państwowe Gospodarstwo Leśne Lasy Państwowe Nadleśnictwo Świdwin z siedzibą w Świdwinie ul. Szczecińska 58 78-300 Świdwin, NIP: 672-000-75-71, reprezentowany przez:
Rafała Grzegorczyka – Nadleśniczego Nadleśnictwa Świdwin

zwana w dalszej części umowy *„Administratorem"*
a

.....
.....
zwana w dalszej części umowy *„Przetwarzającym"*

Mając na uwadze, że:
I. Strony zawarły umowę (dalej: Umowa podstawowa), w związku z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową.

II. Celem umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora.

III. Strony, zawierając Umowę, dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej RODO.

Strony postanowiły zawrzeć Umowę o następującej treści:

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza przetwarzającemu, w trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. z 2014 r. poz. 1182, zwana dalej *„Ustawą"*) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator powierza Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym w niniejszej umowie.

§ 2

Zakres i cel przetwarzania danych

1. Powierzone przez Administratora dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu posiadania danych związanych z prowadzoną działalnością przez Administratora, w sposób zgodny z treścią umowy i jedynie przez czas jej trwania.

2. Przetwarzający będzie przetwarzał powierzone na podstawie umowy, następujące dane osobowe:

Dane zwykłe:

1) imiona, nazwisko;
2) adres zamieszkania lub zameldowania;
3) numer ewidencyjny PESEL;
4) numer telefonu;
5) adres e-mail;
6) adres IP;
7) data urodzenia;
8) NIP;
9) seria i numer dokumentu tożsamości;
10) imiona rodziców;
11) numer rachunku bankowego;

Dane szczególnych kategorii:

12) dokumentacja medyczna;

Dane dzieci:

13) imiona, nazwisko;
14) data urodzenia;
15) adres e-mail;
16) pseudonim;

Dane nieustrukturyzowane:

17) kontent o potencjalnej i prawdopodobnej zawartości danych osobowych (wpisy, dokumenty tekstowe, obrazy, nagrania, filmy).

3. Przetwarzanie danych będzie dotyczyć następujących kategorii osób:
1) pracownicy Administratora i podmiotów stowarzyszonych Administratora,
2) klienci usługi/produktu Administratora określonych w Umowie Podstawowej,
3) osoby, z którymi klienci Administratora wchodzą w interakcje społeczne,
4) kontrahenci (odbiorcy, dostawcy) Administratora i klientów Administratora,
5) odbiorcy korespondencji elektronicznej klientów Administratora.

§ 3

Sposób wykonania umowy w zakresie przetwarzania danych osobowych

1. Przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w szczególności w art. 36 – 39 a RODO.
2. Przetwarzający oświadcza, że zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024):
   1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych;
   2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają poziom bezpieczeństwa określony jako wysoki;
   3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom (Podprzetwarzającym) jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
5. Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy (art. 28 ust. 4 RODO).

§ 4

Odpowiedzialność Przetwarzającego

1. Przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym. Obowiązki Przetwarzającego wynikają m. in. z treści art. 28 ust. 3, art. 25 ust. 1 i 2, art. 30 ust. 2, art. 13 i 14 RODO).
2. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa (art. 82 ust. 3 RODO).

3. Jeżeli Przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym (art. 28 ust. 4 RODO).
4. Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

§ 5

Obowiązki Administratora

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

§ 6

Czas obowiązywania umowy

1. Niniejsza umowa została zawarta na czas obowiązywania Umowy Podstawowej z zastrzeżeniem terminu karencji usunięcia danych wskazanego § 6.
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem trzymiesięcznego okresu wypowiedzenia.

§ 7

1. Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych danych i jest zobowiązany do:

1) usunięcia danych i poinformowania Administratora na piśmie o dacie i sposobie, w jakim usunięto dane,

2) usunięcia wszelkich istniejących kopii lub zwrotu danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie danych.

2. Przetwarzający dokona usunięcia Danych po upływie 180 dni od zakończenia Umowy Podstawowej, chyba że Administrator poleci mu to uczynić wcześniej.

§ 8

Zasady zachowania poufności

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że

konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§ 9

Nadzór

1. Administrator kontroluje sposób przetwarzania powierzonych danych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do:

1) wstępu do pomieszczeń, w których przetwarzane są dane, *oraz*

2) wglądu do dokumentacji związanej z przetwarzaniem danych.

Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania danych oraz udostępnienia rejestrów przetwarzania (z zachowaniem tajemnicy handlowej Przetwarzającego).

2. Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

3. Przetwarzający:

1) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,

2) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzania audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

§ 10

Oświadczenia Stron

1. Administrator oświadcza, że jest Administratorem danych oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.

2. Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętych umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

§ 11

Postanowienia końcowe

1. W razie sprzeczności między postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych między Administratorem

a Przetwarzającym należy regulować przez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

3. Umowa podlega RODO oraz prawu polskiemu.

....

Administrator Przetwarzający

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 2a

REJESTR

Umów powierzenia przetwarzania danych

l.p.	Dane identyfikacyjne strony umowy (nazwa, siedziba, NIP, REGON)	Data zawarcia umowy	Nr umowy	Powierzone czynności		Okres obowiązywania umowy	Dostęp do informacji (należy podać rodzaj informacji)	Uwagi
				Zakres	Miejsce wykonywania			

Załącznik nr 3

Świdwin, dnia.....

UPOWAŻNIENIE nr _____
do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L Nr 119, s. 1) - dalej RODO – nadaję upoważnienie Pani/Panu:

(imię i nazwisko pracownika)

(stanowisko służbowe pracownika)

do przetwarzania w okresie od do danych osobowych w zakresie pełnionych obowiązków służbowych na ww. stanowisku,

(wskazać kategorie danych, które może przetwarzać osoba wymieniona w upoważnieniu lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z niniejszym upoważnieniem oraz z przepisami RODO, prawa polskiego i z ustalonymi przez Pracodawcę zasadami ochrony danych osobowych.

_____

Nadleśniczy

Nadaję identyfikator do przetwarzania ww. danych osobowych w systemie informatycznym: _____.

_____

Administrator sieci

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 4

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Nr upow.	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Komórka organizacyjna/stanowisko	Zakres upoważnienia do przetwarzania danych osobowych	Identyfikator (jeżeli dane są przetwarzane w systemie informatycznym)	Uwagi

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 5

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. (zwane dalej RODO) w związku z przetwarzaniem Pana/i danych osobowych uprzejmie informujemy, że:

1. **Administratorem Twoich danych osobowych (ADO)** jest: Państwowe Gospodarstwo Leśne Lasy Państwowe Nadleśnictwo Świdwin, ul. Szczecińska 58, 78-300 Świdwin.
2. Nasze dane kontaktowe to: Nadleśnictwo Świdwin, ul. Szczecińska 58, 78-300 Świdwin.
3. W sprawach związanych z danymi osobowymi, jesteśmy dostępni pod adresem e-mail: swidwin@szczecinek.lasy.gov.pl lub pod adresem wskazanym w pkt 2.
4. **Cele i podstawy przetwarzania**
   Pana/i dane osobowe przetwarzane będą w celu związanym z nawiązaniem i przebiegiem procesu zatrudnienia, na podstawie art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. b RODO.
5. **Okres przechowywania danych**

Stosownie do tego informujemy, że:

- w przypadku, gdy ADO przetwarza dane osobowe, ponieważ jest to konieczne z uwagi na obowiązujące przepisy prawa, wynika z prawnego obowiązku ciążącego na ADO lub jest związane ze sprawowaniem władzy publicznej, okresy przechowywania danych w tym celu określają przepisy szczególne;
- w pozostałych przypadkach będziemy przechowywać dane osobowe do chwili realizacji zadania, do którego dane zostały zebrane a następnie, jeśli chodzi o materiały archiwalne, przez czas wynikający z przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. 2018 r. poz. 217 ze zm.).

6. **Odbiorcy danych**

Odbiorcami danych osobowych mogą zostać:

- organy nadzorujące przestrzeganie prawa, organy regulacyjne i inne uprawnione organy administracji publicznej;
- podmioty przetwarzające dane osobowe na mocy umów powierzenia przetwarzania danych osobowych.

Dane przekazujemy tylko wówczas i tylko w takim zakresie, w jakim jest to rzeczywiście niezbędne i wymagane w myśl bezwzględnie obowiązujących przepisów prawa i w sposób zgodny z tymi przepisami.

7. **Prawa osób, których dane dotyczą**

Informujemy o przysługującym prawie do:

- dostępu do swoich danych osobowych i żądania ich kopii,
- sprostowania (poprawiania) swoich danych,
- żądania ograniczenia przetwarzania swoich danych,
- przenoszenia danych,
- usunięcia danych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej,
- wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.

8. **Informacja o wymogu/dobrowolności podania danych**

Podanie danych ma charakter dobrowolny, ale jest konieczne do nawiązania stosunku pracy, a w pozostałych przypadkach jest wymagane przepisami prawa.

9. **Zautomatyzowane podejmowanie decyzji**

Zebrane dane nie będą podlegały automatyzacji podejmowania decyzji oraz nie będą profilowane, a także nie będą przekazywane do państw trzecich.

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 6

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. (zwane dalej RODO) w związku z przetwarzaniem Pana/i danych osobowych uprzejmie informujemy, że:

1. **Administratorem Twoich danych osobowych (ADO)** jest: Państwowe Gospodarstwo Leśne Lasy Państwowe Nadleśnictwo Świdwin, ul. Szczecińska 58, 78-300 Świdwin.
2. Nasze dane kontaktowe to: Nadleśnictwo Świdwin, ul. Szczecińska 58, 78-300 Świdwin.
3. W sprawach związanych z danymi osobowymi, jesteśmy dostępni pod adresem e-mail: swidwin@szczecinek.lasy.gov.pl lub pod adresem wskazanym w pkt 2.
4. **Cele i podstawy przetwarzania**

Przetwarzanie danych osobowych osób fizycznych będących naszymi klientami/petentami odbywa się w celu:

- zawarcia lub wykonania zawartej umowy (np. dokonywania zakupów, dzierżawy, najmu – art. 6 ust. 1 lit. b RODO;
- obowiązków wynikających z prawa (np. prawa podatkowego lub przepisów o rachunkowości - art. 6 ust. 1 lit. c RODO;
- wykonywania obowiązków prawnych ciążących na ADO, które realizuje w interesie publicznym lub w ramach sprawowania władzy publicznej (np. nadzór nad lasami nie stanowiącymi własności Skarbu Państwa, zadania Straży i Służby Leśnej w zakresie ochrony lasy przed szkodnictwem) - art. 6 ust. 1 lit. e) RODO;
- ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami (prawnie uzasadnionych interesów realizowanych przez ADO) - art. 6 ust. 1 lit. f RODO.

5. **Okres przechowywania danych**

Stosownie do tego informujemy, że:

- w przypadku, gdy ADO przetwarza dane osobowe na podstawie uzasadnionego interesu, okres przetwarzania trwa do momentu ustania ww. interesu (np. okres przedawnienia roszczeń cywilnoprawnych);
- w przypadku, gdy ADO przetwarza dane osobowe, ponieważ jest to konieczne z uwagi na obowiązujące przepisy prawa, wynika z prawnego obowiązku ciążącego na ADO lub jest związane ze sprawowaniem władzy publicznej, okresy przechowywania danych w tym celu określają przepisy szczególne;
- w przypadku braku konkretnych wymogów prawnych lub umownych, podstawowy okres przechowywania danych w przypadku zapisów i innej dokumentacji dowodowej sporządzonej w trakcie wykonywania umowy wynosi maksymalnie 10 lat;
- w pozostałych przypadkach będziemy przechowywać dane osobowe do chwili realizacji zadania, do którego dane zostały zebrane a następnie, jeśli chodzi o materiały archiwalne, przez czas wynikający z przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. 2018 r. poz. 217 ze zm.).

6. **Odbiorcy danych**

Odbiorcami danych osobowych mogą zostać:

- organy nadzorujące przestrzeganie prawa, organy regulacyjne i inne uprawnione organy administracji publicznej;
- podmioty świadczące usługi w zakresie dochodzenia należności;
- podmioty przetwarzające dane osobowe na mocy umów powierzenia przetwarzania danych osobowych.

Dane przekazujemy tylko wówczas i tylko w takim zakresie, w jakim jest to rzeczywiście niezbędne i wymagane w myśl bezwzględnie obowiązujących przepisów prawa i w sposób zgodny z tymi przepisami.

7. **Prawa osób, których dane dotyczą**

Informujemy o przysługującym prawie do:

- dostępu do swoich danych osobowych i żądania ich kopii,
- sprostowania (poprawiania) swoich danych,
- żądania ograniczenia przetwarzania swoich danych,
- przenoszenia danych,
- usunięcia danych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej,
- wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.

8. **Informacja o wymogu/dobrowolności podania danych**

Podanie danych ma charakter dobrowolny, ale jest konieczne do zawarcia/wykonania umowy, a w pozostałych przypadkach jest wymagane przepisami prawa.

9. **Zautomatyzowane podejmowanie decyzji**

Zebrane dane nie będą podlegały automatyzacji podejmowania decyzji oraz nie będą profilowane, a także nie będą przekazywane do państw trzecich.

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 6a

UWAGA: Informacja zawarta w niniejszej wiadomości lub dowolnym z jej załączników może być chroniona i objęta zakazem jej ujawniania. Jeśli czytelnik niniejszej wiadomości nie jest jej zamierzonym adresatem lub pośrednikiem upoważnionym do jej przekazania adresatowi, niniejszym informujemy, że wszelkie rozprowadzanie, dystrybucja, powielanie niniejszej wiadomości lub jej załączników, bądź inne działanie o podobnym charakterze jest zabronione. Jeżeli otrzymałeś tę wiadomość omyłkowo, proszę bezzwłocznie zawiadomić nadawcę wysyłając odpowiedź na niniejszą wiadomość i usunąć ją z komputera bez otwierania załączników. Dziękujemy. Nadleśnictwo Świdwin

ATTENTION: The information contained in this message or any attachment may be privileged and business confidential and protected from disclosure. If the reader of this message is not the intended recipient or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution, copying of this message or attached files, or any action taken or omitted to be taken in reliance on it, is strictly prohibited. If you have received this communication in error, please notify the sender immediately by replying to the message and deleting it from your computer without opening the attachments. Thank you. Nadleśnictwo Świdwin

Załącznik nr 7

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. (zwane dalej RODO) w związku z przetwarzaniem Pana/i danych osobowych uprzejmie informujemy, że:

1. **Administratorem zebranych danych osobowych** jest: Państwowe Gospodarstwo Leśne Lasy Państwowe Nadleśnictwo Świdwin, ul. Szczecińska 58, 78-300 Świdwin.
2. Wszelkie informacje dotyczące przetwarzania danych osobowych znajdują się na stronie internetowej: www.swidwin.szczecinek.lasy.gov.pl w zakładce RODO.

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 8

Rejestr czynności przetwarzania

Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

NADLEŚNICZY
Rafał Grzegorczyk

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

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Lp.	Nazwa czynności (przetwarzania)	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)	Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)	Kategorie odbiorców (również w państwach trzecich lub organizacjach międzynarodowych)	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju / podmiotu)	Jeśli transfer z art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art. 30 ust. 1 pkt b	Art. 30 ust. 1 pkt c	Art. 30 ust. 1 pkt c			Art. 30 ust. 1 pkt f	Art. 30 ust. 1 pkt a	Art. 30 ust. 1 pkt d	Art. 30 ust. 1 pkt d		Art. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
1	Rekrutacja pracowników pomocniczych, administracyjnych		Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych.	Zgoda osób, których dane dotyczą	Kandydaci do pracy	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Nie dotyczy	Dane nie są przekazywane innym podmiotom	System Kadry, Dokumentacja papierowa	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana	Nie dotyczy	Nie dotyczy
2	Prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy	Samodzielne stanowisko ds. kadr	Prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy	Pracownicy pomocniczy (recepcjoniści, sprzątacze, pracownicy gospodarczy), administracyjni	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem Pracy	• Umowa o pracę, • Przepis prawa. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) - w szczeg. art. 22 § ind. 1 w związku z art. 94 pkt 9a i 9b	Pracownik	50 lat (art. 51u ust 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.))	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	System Kadry, Dokumentacja papierowa	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana	Nie dotyczy	Nie dotyczy
3	Zgłoszenie pracowników i członków ich rodzin do ZUS, ich aktualizacja i przekazywanie danych o zwolnieniach.	Samodzielne stanowisko ds. kadr	Zgłoszenie pracownika i członków jego rodziny do ZUS, ich aktualizacja oraz przekazywanie informacji o zwolnieniach	Pracownicy pomocniczy (recepcjoniści, sprzątacze, pracownicy gospodarczy), administracyjni	Dane identyfikacyjne, dane adresowe, dane o Oddziale NFZ oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS ZZA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA - zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zwolnienia lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny	• Przepis prawa Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a	Pracownik	50 lat (art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2017 r., poz. 1383))	Nie dotyczy	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Systemy Kadry, Płacowe, Dokumentacja papierowa	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana	Nie dotyczy	Nie dotyczy
4	Prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń, naliczanie obciążeń oraz naliczanie składek do ZUS	Samodzielne stanowisko ds. płac	Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS	Pracownicy pomocniczy (recepcjoniści, sprzątacze, pracownicy gospodarczy), administracyjni	Dane identyfikacyjne, dane adresowe, dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach (składki związkowe, zajęcia komornicze itp.) numery kont dla przelewów bankowych pracownika	Umowa o pracę, Przepis prawa • Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r., poz. 108 t.j.) Dział III Wynagrodzenie; ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2017 r., poz. 1778 t.j.) - art. 1, 6 oraz 6a. • Ustawa z dnia 26 stycznia 1982 - Karta Nauczyciela (Dz. U. z 2017 r., poz. 1189 t.j.) - Rozdział 5	Pracownik	50 lat (art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2017 r., poz. 1383))	Nie dotyczy	Nie dotyczy	Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe.	System Płace, Płatnik Dokumentacja papierowa	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.	Po przeprowadzeniu oceny ryzyka podjęto decyzję, że ocena skutków dla ochrony danych nie jest wymagana.	Nie dotyczy	Nie dotyczy

NADLEŚNICZY
Rafał Grzegorczyk

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 1

ISTOTA NARUSZENIA DANYCH OSOBOWYCH

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1. nieautoryzowany dostęp do danych,
2. nieautoryzowane modyfikacje lub zniszczenie danych,
3. udostępnienie danych nieautoryzowanym podmiotom,
4. nielegalne ujawnienie danych,
5. pozyskiwanie danych z nielegalnych źródeł.

§ 2

POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt osobie upoważnionej przez nadleśniczego do prowadzenia nadzoru nad bezpieczeństwem danych (dalej „osoba upoważniona").
2. Typowe sytuacje, gdy pracownik powinien powiadomić przełożonego:
   - I.1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   - I.2. dokumentacja jest niszczona bez użycia niszczarki;
   - I.3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
   - I.4. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
   - I.5. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,
   - I.6. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;

I.7. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
I.8. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
I.9. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
I.10. telefoniczne próby wyłudzenia danych osobowych;
I.11. kradzież komputerów, smartfonów, przenośnych pamięci USB lub twardych dysków z danymi osobowymi;
I.12. utrata kontroli nad kopią danych osobowych;
I.13. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
I.14. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
I.15. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
I.16. hasła do systemów przechowywane są w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby upoważnionej.

§ 5

Administrator Systemu Informatycznego/Sieci jest zobowiązany do informowania osoby upoważnionej o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Osoba upoważniona podejmuje następujące kroki:
1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7

Osoba upoważniona dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport – Załącznik nr 1.

§ 8

Osoba upoważniona zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

§ 9

NARUSZENIE DANYCH OSOBOWYCH - ODPOWIEDZIALNOŚĆ

Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 10

ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

1. W przypadku naruszenia ochrony danych osobowych, osoba upoważniona bez zbędnej zwłoki zgłasza je Urzędowi ochrony danych w terminach i sposobach określonych w odpowiednich aktach prawnych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Osoba upoważniona prowadzi ewidencję naruszeń danych osobowych – Załącznik nr 2.
3. Zgłoszenie, o którym mowa w ust. 1 wraz z potwierdzeniem przesłania należy przechowywać łącznie z rejestrem o którym mowa w ust 2, w którym naruszenie zostało zarejestrowane.

§ 11

ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, osoba upoważniona bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera informacje o przesłaniu zgłoszeniu o którym mowa w § 10 ust. 1.

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   3.1. wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

3.2. zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 1

RAPORT Z NARUSZENIA OCHRONY DANYCH

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

   .....

   (imię, nazwisko, stanowisko służbowe,):

3. Lokalizacja zdarzenia .....

   (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

   .....

5. Podjęte działania:

   .....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

   .....

7. Postępowanie wyjaśniające i naprawcze:

   .....

.....
(podpis pracownika)

.....
(data i podpis Inspektora ochrony danych)

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 2

EWIDENCJA NARUSZEŃ W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

l.p.	Data naruszenia	Data stwierdzenia naruszenia	Opis naruszenia	Skutki naruszenia	Opis zastosowanych środków zaradczych	Data dokonania zgłoszenia organowi nadzorczemu (jeżeli dotyczy) lub uzasadnienie dla faktu niedokonania zgłoszenia	Data poinformowania osób, których dane dotyczą (jeżeli dotyczy) lub uzasadnienie dlaczego odstąpiono od poinformowania w/w osób	Forma w jakiej została przekazana informacja osobom, których dane dotyczą (jeżeli dotyczy)

*należy każdorazowo dołączyć treść zgłoszenia do organu nadzorczego oraz informacji przekazanej podmiotom danych

NADLEŚNICZY
Rafał Grzegorczyk

Załącznik nr 10

POLITYKA SILP

(Zarządzenie nr 312 DGLP w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego PGL LP z dnia 19 września 2017 roku)

NADLEŚNICZY
Rafał Grzegorczyk