Zarządzenie Nr 5/25
Dyrektora Zespołu Parków Krajobrazowych
Województwa Śląskiego
z dnia 18 lutego 2025 r.

w sprawie: Procedury bezpieczeństwa przetwarzania danych osobowych w Zespole Parków Krajobrazowych Województwa Śląskiego.

Na podstawie 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, str. 1) oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000 z późn. zm.)

zarządzam, co następuje:

§ 1

Wprowadzam Procedury Bezpieczeństwa Informacji w zakresie danych osobowych w zakresie przetwarzania danych osobowych w Zespole Parków Krajobrazowych Województwa Śląskiego, które zostaną opisane w następujących załącznikach:

1. Polityka Bezpieczeństwa Informacji w zakresie danych osobowych stanowiąca **Załącznik nr 1 do Zarządzenia;**
2. Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, stanowiąca **Załącznik nr 2 do Zarządzenia**;
3. Analiza ryzyka i skutków przy przetwarzaniu danych osobowych, stanowiąca **Załącznik nr 3 do Zarządzenia** z odniesieniem do arkusza analizy ryzyka (Excel);
4. Procedura postępowania z incydentami i naruszeniami ochrony danych osobowych, stanowiąca **Załącznik nr 4 do Zarządzenia**;
5. Zasady zachowania poufności i ochrony danych osobowych, stanowiące **Załącznik nr 5 do Zarządzenia**;
6. Ewidencja osób upoważnionych do przetwarzania danych osobowych stanowiąca **Załącznik nr 6 do Zarządzenia**;
7. Rejestr czynności przetwarzania danych osobowych, stanowiący **Załącznik nr 7 do Zarządzenia**.
8. Rejestr umów powierzenia przetwarzania danych osobowych, stanowiący **Załącznik nr 8 do Zarządzenia.**

§ 2

1. Celem opracowania Procedury bezpieczeństwa przetwarzania danych osobowych jest określenie zasad ochrony danych osobowych przetwarzanych w ZPKWŚ.
2. Zasady określone w Procedurach bezpieczeństwa przetwarzania danych osobowych mają obowiązek stosować wszystkie osoby upoważnione przez Administratora Danych do przetwarzania danych osobowych, niezależnie od formy ich zatrudnienia.
3. Utrzymanie bezpieczeństwa przetwarzanych przez ZPKWŚ danych osobowych oraz informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności na wysokim poziomie zapewniającym bezpieczeństwo.
4. Aktualność procedur „Ewidencja osób upoważnionych do przetwarzania danych osobowych”, „Rejestr czynności przetwarzania danych osobowych” oraz „Rejestr umów

powierzenia przetwarzania danych osobowych” winna być weryfikowana na zgodność ze stanem rzeczywistym w każdym kwartale danego roku przez kierowników działów i oddziałów. W przypadku stwierdzenia konieczności aktualizacji przedmiotowych procedur, o konieczności wprowadzenia zmian i ich zakresie zostanie powiadomiony pisemnie Inspektor Ochrony Danych.

§ 3

1. Odpowiedzialnym za treści i uprawnionym do wnoszenia zmian w niniejszym Zarządzeniu jest Dyrektor ZPKWŚ.
2. Traci moc Zarządzenie Nr 3/21 Dyrektora ZPKWŚ z dnia 5 lutego 2021r., w sprawie: procedury bezpieczeństwa przetwarzania danych osobowych w Zespole Parków Krajobrazowych Województwa Śląskiego.

§ 4

Wykonanie Zarządzenia powierzam Inspektorowi Ochrony Danych, pracownikom i współpracownikom przetwarzającym dane osobowe w ZPKWŚ.

§ 5

Za nadzór nad realizacją Zarządzenia w ZPKWŚ oraz aktualizację jego zapisów odpowiada Dyrektor Zespołu Parków Krajobrazowych Województwa Śląskiego.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

SPIS TREŚCI

Załącznik nr 1
do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Polityka Bezpieczeństwa Informacji w zakresie danych osobowych

Rozdział 1
Definicje

§ 1

Przez użyte w Polityce Bezpieczeństwa Informacji w zakresie danych osobowych określenia należy rozumieć:

1. **Zespół Parków Krajobrazowych Województwa Śląskiego** – zwany dalej „ZPKWŚ”,
2. **Administrator Danych Osobowych –** Zespół Parków Krajobrazowych Województwa Śląskiego reprezentowany przez Dyrektora ZPKWŚ, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
3. **Inspektor Ochrony Danych** – osoba wyznaczona przez Administratora Danych, która będzie nadzorować przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych, tj. stosowanie środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną,
4. **ustawa** – ustawa z dnia 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000),
5. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/,
6. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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,

7. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
8. **przetwarzane danych –** operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,
9. **system informatyczny –** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
10. **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
11. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
12. **Pomoc informatyczna** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
13. **odbiorca –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
14. **strona trzecia/odbiorca danych –** osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
15. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
16. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
17. **uwierzytelnienie –** działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Rozdział 2
Postanowienia ogólne

§ 2

Celem Polityki bezpieczeństwa informacji w zakresie danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w ZPKWŚ, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących przepisów o ochronie danych osobowych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia: fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w ZPKWŚ rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.
2. Każda osoba przetwarzająca dane osobowe zobowiązana jest do ich zabezpieczenia oraz przetwarzania w sposób uniemożliwiający zapoznanie się z nimi przez osoby nieuprawnione.
3. Dane osobowe należy zachować w tajemnicy zarówno w czasie trwania stosunku pracy/współpracy, jak i po jego ustaniu.
4. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
5. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,
   5) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   6) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

Rozdział 3
Zadania i obowiązki

§ 5

1. Administratorem przetwarzanych danych osobowych jest Zespół Parków Krajobrazowych Województwa Śląskiego reprezentowany przez Dyrektora ZPKWŚ.
2. Do zadań i obowiązków **Administratora Danych Osobowych** należy:
   1) ustanowienie zasad przetwarzania danych osobowych w ZPKWŚ,
   2) decydowanie o celach i środkach przetwarzania danych osobowych,
   3) wdrożenie odpowiednich środków organizacyjno – technicznych, zapewniających skuteczną ochronę praw osób, których dane dotyczą, zarówno na etapie projektowania danego przedsięwzięcia, jak i w czasie jego trwania (zgodnie z art. 24, 25 i 32 RODO),
   4) ustanowienie inspektora ochrony danych w ZPKWŚ,
   5) podpisywanie umów powierzenia z podmiotami zewnętrznymi, którym ZPKWŚ zamierza powierzyć dane osobowe. Powierzenie przetwarzania danych, w imieniu i na rzecz ZPKWŚ, odrębnemu podmiotowi może przebiegać tylko i wyłącznie z zachowaniem zasad przewidzianych w RODO,
   6) w przypadku naruszenia ochrony danych osobowych, administrator przy pomocy Inspektora Ochrony Danych, bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą.

3. Administrator danych osobowych upoważniając określone osoby do przetwarzania danych osobowych zachowuje zasadę, że dostęp do danych osobowych będą miały tylko te osoby, którym jest to niezbędne do realizacji powierzonych zdań.
4. Do przetwarzania danych osobowych mogą być dopuszczone osoby, które:
   1) posiadają upoważnienie do przetwarzania danych osobowych,
   2) posiadają potrzebę dostępu do danych osobowych, wynikającą z konieczności realizacji zadań i obowiązków na danym stanowisku,
   3) zostały przeszkolone w zakresie przepisów dotyczących ochrony danych osobowych oraz zasad przetwarzania danych osobowych, określonych w niniejszej Polityce.

§ 6

1. **Inspektor Ochrony Danych** ma następujące zadania i obowiązki:
   1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
   2) monitorowanie przestrzegania rozporządzenia Parlamentu Europejskiego i Rady (UE), innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
   3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia Parlamentu Europejskiego i Rady (UE),
   4) współpraca z organem nadzorczym,
   5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
   6) monitorowanie i opiniowanie organizacji bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami rozporządzenia Parlamentu Europejskiego i Rady (UE) i ustawy o ochronie danych osobowych,
   7) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi,
   8) monitorowanie przeprowadzenia oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych – w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych,
   9) wsparcie w identyfikacji i analizie ryzyka utraty bezpieczeństwa danych osobowych przetwarzanych w ZPKWŚ oraz monitorowanie wdrożonych zabezpieczeń w celu ochrony danych osobowych,
   10) nadzorowanie prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych przy współpracy z administratorem danych osobowych,
   11) nadzór nad bezpieczeństwem danych osobowych,
   12) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
   13) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
   14) zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych osobowych,
b) nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych,
c) zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

15) nadzór nad prowadzeniem rejestru czynności na podstawie art. 30 Rozporządzenia Parlamentu Europejskiego i rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE Nr 119).

2. Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

§ 7

1. **Pomoc informatyczna** odpowiedzialna jest za:
   1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   2) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   3) instalacje i konfiguracje oprogramowania systemowego, sieciowego,
   4) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
   5) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
   7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
   8) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
   10) przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
   11) wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
   12) zarządzanie licencjami, procedurami ich dotyczącymi,
   13) prowadzenie profilaktyki antywirusowej,
   14) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji w systemach teleinformatycznych,
   15) zgłaszanie do inspektora ochrony danych każdego incydentu bezpieczeństwa danych osobowych lub zdarzeń potencjalnie naruszających bezpieczeństwo danych osobowych przetwarzanych w systemach teleinformatycznych ZPKWŚ,
   16) udział w identyfikacji i analizie ryzyka utraty bezpieczeństwa danych osobowych przetwarzanych w ZPKWŚ oraz monitorowanie wdrożonych zabezpieczeń dla systemów teleinformatycznych ZPKWŚ w celu ochrony danych osobowych i informacji.

2. Praca Pomocy informatycznej jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych oraz Procedury bezpieczeństwa przetwarzania danych osobowych w ZPKWŚ przez Administratora Danych Osobowych.

§ 8

1. Zadania **każdego pracownika i współpracownika** w ZPKWŚ, związane z ochroną danych osobowych:
   1) identyfikacja danych osobowych przetwarzanych w komórce organizacyjnej/na stanowisku pracy i zgłaszanie zbiorów danych osobowych do inspektora ochrony danych,
   2) identyfikacja, ocena i szacowanie ryzyka utraty bezpieczeństwa danych osobowych przetwarzanych w ZPKWŚ,
   3) ochrona zasobów danych osobowych przetwarzanych w ZPKWŚ przed ich utratą, nieuprawnionym użyciem lub ich zniszczeniem,
   4) zachowanie szczególnej staranności przy gromadzeniu i przetwarzaniu danych osobowych, aby dane te były:
      a. przetwarzane zgodnie z prawem,
      b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawanie dalszemu przetwarzaniu niezgodnemu z tymi celami,
   5) zgłaszanie inspektorowi ochrony danych wszelkich zauważonych nieprawidłowości dotyczących ochrony danych osobowych przetwarzanych w systemach informatycznych i tradycyjnej papierowej formie,
   6) poprawne korzystanie z aplikacji zgodnie z powierzonymi obowiązkami służbowymi,
   7) informowanie interesantów, o administratorze danych osobowych, inspektorze ochrony danych oraz prawach związanych z ochroną danych osobowych, zgodnie z klauzulą informacyjną zawartą w **Załączniku nr 1 do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych,**
   8) informowanie (pracownik ds. kadr) nowozatrudnionych pracowników o administratorze danych osobowych, inspektorze ochrony danych oraz prawach związanych z ochroną danych osobowych, zgodnie z klauzulą informacyjną zawartą w **Załączniku nr 2 do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych,**
   9) informowanie wykonawców (zleceniobiorców) o administratorze danych osobowych, inspektorze ochrony danych oraz prawach związanych z ochroną danych osobowych, zgodnie z klauzulą informacyjną zawartą w **Załączniku nr 3 do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych,**
   10) informowanie opiekunów dzieci uczestniczących we wszelkich formach edukacji ekologicznej o administratorze danych osobowych, inspektorze ochrony danych oraz prawach związanych z ochroną danych osobowych, zgodnie z klauzulą informacyjną zawartą w **Załączniku nr 4 do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych,**
   11) informowanie kandydatów w procesie rekrutacji o administratorze danych osobowych, inspektorze ochrony danych oraz prawach związanych z ochroną danych osobowych, zgodnie z klauzulą informacyjną zawartą w **Załączniku nr 3 do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych,**
   12) wszyscy pracownicy ZPKWŚ są zobowiązani zachowywać czystość biurka, aby w miejscu pracy nie znajdowały się dokumenty z danymi osobowymi i/lub danymi wrażliwymi, które byłyby łatwo dostępne dla niepowołanych osób. Jest to niezwykle ważne, szczególnie w dyrekcji, sekretariacie, księgowości oraz kadrach.

Rozdział 4
Zakres stosowania

§ 9

1. W ZPKWŚ przetwarzane są dane osobowe pracowników, kandydatów do pracy, kontrahentów/interesantów/uczestników wydarzeń/zleceniobiorców zebrane w zbiorach danych osobowych.
2. Dane te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Przetwarzanie danych osobowych (zgodnie z art. 6 ust. 1 lit. a-f RODO) jest dopuszczalne tylko wtedy gdy:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów zgodnie z klauzulą informacyjną zawartą w **Załączniku nr 8 do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych,**
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych.
4. Polityka bezpieczeństwa informacji w zakresie danych osobowych zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w § 13.

§ 10

Politykę Bezpieczeństwa Informacji w zakresie danych osobowych stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemie: Probit, Płatnik, Fakturownia online, Microsoft Office,
2) wszystkich informacji dotyczących danych: pracowników, zleceniobiorców, stażystów, kontrahentów, interesantów, osób ubiegających się o pracę/staż/ praktykę,
3) odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia przetwarzania danych firma świadcząca usługi z zakresu BHP, Probit, radca prawny, serwer poczty e-mail, dziennik korespondencyjny, Agencje Ochrony Mienia – Będzin, lub w oparciu o odrębne przepisy, np.: specjalistyczna przychodnia lekarska, ZUS,
4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5) rejestru osób trzecich /np. pracownicy/ mających upoważnienia Administratora Danych Osobowych do przetwarzania danych osobowych,

6) innych dokumentów zawierających dane osobowe.

§ 11

1. Zakresy ochrony danych osobowych określone przez Politykę Bezpieczeństwa Informacji w zakresie danych osobowych oraz inne z nią związane dokumenty mają zastosowanie do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz zbiorów papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   3) wszystkich pracowników, stażystów i innych osób mających dostęp do danych podlegających ochronie.
2. Do stosowania zasad określonych przez Politykę Bezpieczeństwa Informacji w zakresie danych osobowych oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 5
Obowiązki informacyjne Administratora Danych Osobowych

§ 12

1. W przypadku zbierania danych od osoby, której te dane dotyczą Administrator, zgodnie z treścią art. 13 RODO, podaje jej wszystkie następujące informacje:
   1) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
   2) dane kontaktowe inspektora ochrony danych,
   3) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania,
   4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
   5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   6) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   7) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   8) jeżeli przetwarzanie odbywa się na podstawie zgody – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   9) informacje o prawie wniesienia skargi do organu nadzorczego,
   10) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
   11) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 Rozporządzenia UE, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. W przypadku zbierania danych nie od osoby, której te dane dotyczą Administrator jest zobowiązany, zgodnie z art. 14 RODO, poinformować tę osobę bezpośrednio po utrwaleniu danych dodatkowo o:
   1) źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych,
   2) kategoriach odnośnych danych osobowych.
3. Obowiązków określonych w ust. 1 i 2 nie stosuje się, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami.
4. Przykładowa treść klauzul informacyjnych stanowi załączniki do 1-4 do niniejszej Polityki.
5. Zgodnie z treścią art. 15-21 RODO osoba, której dane dotyczą, jest uprawniona do:
   1) uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do tych danych,
   2) żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe,
   3) żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych (wyłącznie w określonych sytuacjach),
   4) żądania od administratora ograniczenia przetwarzania (wyłącznie w określonych sytuacjach),
   5) otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła administratorowi, a także ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe (wyłącznie w określonych sytuacjach),
   6) wniesienia sprzeciwu w dowolnym momencie wobec przetwarzania jej danych osobowych – z przyczyn związanych z jej szczególną sytuacją (wyłącznie w określonych sytuacjach).

Rozdział 6
Postępowanie w przypadku incydentów bezpieczeństwa danych osobowych

§ 13

1. Wszyscy pracownicy i współpracownicy ZPKWŚ zobowiązani są do natychmiastowego zgłaszania Administratorowi Danych Osobowych i/lub Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu incydentów związanych z naruszeniem bezpieczeństwa przetwarzania danych osobowych.
2. Inspektor Ochrony Danych, w ciągu 72 godzin od momentu zgłoszenia naruszenia, dokonuje jego oceny, zasadności oraz ustalenia stanu faktycznego przy wsparciu Pomocy informatycznej oraz innych osób, których wiedza lub wyjaśnienia mogą być pomocne.
3. W przypadku ustalenia powyższych informacji, Inspektor Ochrony Danych przekazuje rekomendację do Administratora Danych.
4. Administrator, bez zbędnej zwłoki, jednakże nie później niż w ciągu 72 godzin od momentu wykrycia naruszenia, zgłasza to naruszenie, wraz z ustaleniami Inspektora Ochrony Danych, organowi nadzorczemu. Zgłoszenie odbywa się zgodnie z wymogami art. 33 RODO.
5. Nie jest wymagane dokonanie zgłoszenia, o którym mowa w ust. 3, o ile jest mało prawdopodobne, by dane naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych.

6. Inspektor Ochrony Danych zobowiązany jest prowadzić rejestr incydentów związanych z naruszeniem bezpieczeństwa przetwarzania danych osobowych.

Rozdział 7
Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

§ 14

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa Zarządzenie Dyrektora ZPKWŚ w sprawie: Systemu Administracyjno- Gospodarczego ZPKWŚ.

Rozdział 8
Powierzenie przetwarzania danych

§ 15

1. Zgodnie z treścią art. 28 RODO, administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi, który będzie dokonywał przetwarzania w imieniu i na rzecz administratora.
2. Powierzenie, o którym mowa w ust. 1, może zostać dokonane wyłącznie do podmiotu przetwarzającego, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Tak aby przetwarzanie spełniało wymogi RODO, i zapewniało ochronę praw osób, których dane dotyczą.
3. Powierzenie przetwarzania danych osobowych może odbywać się wyłącznie na podstawie umowy lub innego instrumentu prawnego, wiążącego administratora z podmiotem przetwarzającym dane. Zapisy lub umowa, o których mowa w zdaniu poprzednim, muszą zawierać co najmniej informacje określone w art. 28 ust. 3 RODO.
4. Załącznik **nr 5 do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych** przedstawia wzór umowy powierzenia przetwarzania danych.
5. Podmiot przetwarzający może skorzystać z usług innego podmiotu przetwarzającego wyłącznie po uzyskaniu pisemnej zgody administratora danych.
6. Każdorazowo o fakcie lub potrzebie zawarcia umowy powierzenia przetwarzania danych osobowych należy powiadomić pisemnie Inspektora Ochrony Danych.

Rozdział 9
Nadawanie upoważnień do przetwarzania danych osobowych

§ 16

1. Dane osobowe znajdujące się w zbiorach ZPKWŚ mogą przetwarzać wyłącznie osoby posiadające upoważnienie Administratora Danych Osobowych oraz wpisane w ewidencję osób upoważnionych do ich przetwarzania.
2. Imienne upoważnienie do dostępu i przetwarzania danych osobowych nadaje i odwołuje Administrator Danych Osobowych.

3. Zakres upoważnienia winien wynikać z zakresu zadań delegowanych do realizacji osobie upoważnianej. Zakres upoważnienia w szczególności określa zbiory/procesy co, do których ma ono zastosowanie, a także wskazuje czynności przetwarzania danych, które upoważniona osoba w ramach procesu ma prawo wykonywać.
4. Przesłanki, które winny wstrzymać proces nadania uprawnień to w szczególności:
   - wobec osoby w wyniku zakończonych wcześniejszych postępowań wydano zakaz przetwarzania danych osobowych,
   - wnioskowany zakres upoważnienia do przetwarzanych danych osobowych jest niezgodny z zakresem zadań danej osoby,
   - wobec osoby prowadzone jest postępowanie wyjaśniające w zakresie rażących zaniedbań lub niedopełnienia obowiązków w zakresie prawidłowości przetwarzania danych osobowych.
5. W przypadku wystąpienia przesłanek, o których mowa wyżej, Inspektor Ochrony Danych podejmuje kroki w celu ich wyeliminowania lub informuje o nich Administratora Danych Osobowych celem wydania warunkowej zgody o nadanie uprawnień.
6. Upoważnienie do przetwarzania danych nadaje się z chwilą zatrudnienia osoby w ZPKWŚ, zmiany stanowiska bądź zmian w zakresie kategorii przetwarzanych danych.
7. O każdym zatwierdzonym przypadku nadania lub cofnięcia upoważnienia do przetwarzania danych osobowych przetwarzanych w systemach teleinformatycznych pracownik ds. kadr informuje Pomoc Informatyczną o konieczności dostosowania przez nią uprawnień w systemach, które dokumentuje papierowo lub elektronicznie.
8. Za całość procesu związanego z nadawaniem / cofaniem upoważnień do przetwarzania danych odpowiedzialny jest pracownik ds. kadr.

§ 17

1. Udostępnianie danych osobowych przez ZPKWŚ wynika jedynie z obowiązujących przepisów prawa. Złożony wniosek winien zawierać obowiązującą podstawę prawną do udostępnienia danych osobowych.
2. Osoby upoważnione, do których wpływają wnioski o udostępnienie danych, obowiązani są każdorazowo do przeanalizowania możliwości oraz zakresu udostępnienia danych osobowych w uzgodnieniu z Inspektorem Ochrony Danych.
3. W celu zapewnienia przez ZPKWŚ kontroli nad tym, komu dane są przekazywane, udostępnienie danych powinno odbywać się, co do zasady w formie pisemnej, co pozwoli w szczególności na udokumentowanie podstawy prawnej udostępnienia danych i podmiotu, który o to się zwróci.
4. Zabrania się:
   a) przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować,
   b) przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

Rozdział 10
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 18

1. Środki organizacyjno – techniczne są dostosowane do charakteru, zakresu, kontekstu oraz celu przetwarzania danych, uwzględnia ryzyko naruszenia praw i wolności osób fizycznych, a także stan wiedzy technicznej i koszty wdrożenia określonego rozwiązania.

2. Zabezpieczenia organizacyjne:
   1) opracowano i wdrożono **Politykę Bezpieczeństwa Informacji w zakresie danych osobowych** w ZPKWŚ,
   2) sporządzono i wdrożono **Instrukcję Zarządzania Systemem Informatycznym** służącym do przetwarzania danych osobowych w ZPKWŚ,
   3) stworzono **Procedurę postępowania w przypadku naruszenia ochrony danych osobowych,**
   4) został powołany Inspektor Ochrony Danych,
   5) wprowadzono „Ewidencję osób upoważnionych do przetwarzania danych osobowych" - § 6 pkt 1, p.pkt11 Polityki Bezpieczeństwa Informacji w zakresie danych osobowych,
   6) opracowano i bieżąco prowadzi się rejestr czynności przetwarzania - § 6 pkt 1, p.pkt16 Polityki Bezpieczeństwa Informacji w zakresie danych osobowych;
   7) dokumentowane są incydenty i naruszenia danych osobowych,
   8) prowadzone jest ewidencja obszarów przetwarzania danych,
   9) wprowadzono schemat przepływu informacji pomiędzy poszczególnymi systemami zgodnie z załącznikiem nr 6,
   10) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,
   11) osoby upoważnione przez administratora danych, przetwarzające dane osobowe, zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
   12) osoby upoważnione przez administratora danych, przetwarzające dane osobowe, obowiązane zostały do zachowania ich w tajemnicy,
   13) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
   14) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych i odpowiednią poufność,
   15) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści,
   16) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzania danych osobowych.
2. Zabezpieczenia techniczne:
   1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą urządzenia klasy UTM oraz bezpiecznego systemu bezprzewodowego (z wydzieloną strefą ogólnodostępną), chroniącego przed dostępem z zewnątrz przez osoby nieupoważnione,
   2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   3) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania,
   4) użyto system Firewall do ochrony dostępu do sieci komputerowej,
   5) prowadzona jest rejestracja i monitorowanie ruchu wychodzącego i przychodzącego w punkcie styku z teleinformatyczną siecią publiczną,
   6) zapewniono zapasowe łącze internetowe,

3. Środki ochrony fizycznej:
   1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem, czujnikami ruchu, monitoringiem, oraz zewnętrzną firmą ochroniarską,
   2) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
   3) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach lub w szafach pancernych,
   4) pomieszczenie Działu Księgowego posiada rolety antywłamaniowe.
   5) pomieszczenie Działu Kadrowego posiada rolety antywłamaniowe.
   6) dane osobowe oraz wrażliwe są głównie przechowywane w szafach stalowych lub posiadają odpowiednie zabezpieczenia antywłamaniowe.
   7) pomieszczenia, w których przetwarzane są zbiory danych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolno stojącej gaśnicy,
   8) opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używanych aktualnie zbiorów danych np. wygaszacz ekranu chroniony hasłem.

Rozdział 11
Zasady funkcjonowania monitoringu wizyjnego

§ 19

1. Monitoring wizyjny jest stosowany w celu:
   1) zapewnienie bezpieczeństwa pracownikom,
   2) ochrony mienia pracodawcy,
   3) wykrywania zachowań szkodzących pracownikom lub narażających pracodawcę na straty.
2. Dokumentacja monitoringu wizyjnego powinna określać:
   1) osoby sprawujące nadzór nad monitoringiem,
   2) lokalizacje objęte monitoringiem,
   3) miejsca instalacji kamer,
   4) cele monitoringu,
   5) części składowe systemu monitoringu,
   6) okres przechowywania danych,
   7) warunki udostępnienia zapisu z monitoringu.
3. Udostępnienie zapisu z monitoringu może nastąpić:
   1) gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych osobowych w przypadku toczących się postępowań, czynności prowadzonych przez podmioty upoważnione na podstawie przepisów prawa (w szczególności w przypadkach zgłaszania się o udostępnienie nagrań przez Policję, Prokuraturę),
   2) na podstawie zgody osób, których wizerunek zostanie ujawniony na nagraniach,
   3) firmom trzecim zajmującym się na podstawie stosowania umowy, ochroną mienia pracodawcy, z którymi dodatkowo zostanie zawarta umowa o powierzeniu przetwarzania danych osobowych.
4. Czynności związane z przetwarzaniem danych osobowych ujawnionych na nagraniach z monitoringu wizyjnego powinny być zawarte w Rejestrze przetwarzania danych osobowych.

5. Administrator danych osobowych ma obowiązek poinformowania pisemnie pracowników o planowanym uruchomieniu monitoringu wizyjnego. W przypadku nowych pracowników realizacja tego obowiązku powinna nastąpić również pisemnie przed dopuszczeniem ich do pracy.
6. W lokalizacjach, w których funkcjonuje monitoring wizyjny konieczne jest umieszczenie tablicy informacyjnej o tym fakcie. Tablica powinna być umieszczona w okolicach wejścia do danego obiektu.
7. Wzór klauzuli informacyjnej dotyczącej monitoringu wizyjnego przedstawia **Załącznik nr 7** do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych.

Rozdział 12
Sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych

§ 20

1. Corocznie do końca lutego Inspektor Ochrony Danych Osobowych, przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych i przekazuje do administratora danych osobowych – Dyrektora ZPKWŚ.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 13
Postanowienia końcowe

§ 21

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym, w którym przetwarzane są dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Procedurą bezpieczeństwa przetwarzania danych osobowych w ZPKWŚ,
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

Załącznik nr 1
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Klauzula informacyjna

„Zgodnie z art. 13 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) dalej RODO informujemy, że:

1. Administratorem Pana/i danych osobowych jest:
Zespół Parków Krajobrazowych Województwa Śląskiego w Katowicach z siedzibą w Będzinie reprezentowany przez Dyrektora ZPKWŚ,
ul. I. Krasickiego 25, 42-500 w Będzinie

2. Kontakt z Inspektorem Ochrony Danych w Zespole Parków Krajobrazowych Województwa Śląskiego jest możliwy pod adresem email lub na adres siedziby Administratora danych *(adres mailowy, inne dane kontaktowe)*

3. Pana/i dane osobowe przetwarzane są w celu *(cel np. rekrutacja)* **na podstawie** *(podstawa prawna np. art.6 ust.1 lit.c - obowiązek prawny administratora + przepis szczególny)*

4. Dane osobowe mogą być przekazywane innym organom i podmiotom wyłącznie na podstawie obowiązujących przepisów prawa. Pani/Pana dane mogą zostać przekazane następującym podmiotom: …….

5. Pana/i dane osobowe będą przetwarzane przez okres *(np. do zakończenia rekrutacji lub wynikający z instrukcji kancelaryjnej)*

6. Posiada Pan/i prawo do: dostępu do treści swoich danych i ich poprawiania, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych , wniesienia sprzeciwu, cofnięcia zgody na przetwarzanie *(wpisujemy te prawa, które mają zastosowanie)*

7. Ma Pan/i prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych Pana/ią dotyczących naruszałoby przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 roku

8. Pani/Pana dane nie będą poddawane profilowaniu.

9. ZPKWŚ nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

10. Podanie danych osobowych jest *(np. obowiązkiem ustawowym, warunkiem zawarcia umowy)* **Jest Pan/i zobowiązany/a do podania danych** *(np. określonych w formularzu)***, a konsekwencją niepodania danych będzie** *(wskazać konsekwencje)"*

Załącznik nr 2
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Klauzula informacyjna
przekazywana nowozatrudnionym pracownikom

Zgodnie z treścią art. 13 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 RODO informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Zespół Parków Krajobrazowych Województwa Śląskiego w Katowicach z siedzibą w Będzinie, ul. I. Krasickiego 25, 42-500 Będzin.
2. Z Inspektorem Ochrony Danych można kontaktować się mailowo, pod adresem iod@zpk.com.pl lub pocztą tradycyjną pod adresem kontaktowy Administratora danych.
3. Pani/Pana dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. a, b, c oraz art. 9 ust. 2 lit. b, h RODO, w celu związanym z nawiązaniem i przebiegiem procesu zatrudnienia.
4. Pani/Pana dane osobowe będą przechowywane w trakcie okresu zatrudnienia w Zespole Parków Krajobrazowych Województwa Śląskiego oraz na potrzeby archiwizacji dokumentacji pracowniczej według okresów wskazanych w przepisach szczegółowych.

5. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu.
6. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
7. Podanie przez Pana/Panią danych osobowych jest wymagane dla celów związanych z nawiązaniem i przebiegiem Pani/Pana zatrudnienia.
8. Pani/Pana dane nie będą poddawane profilowaniu. Zespół Parków Krajobrazowych Województwa Śląskiego nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
9. Dane osobowe są przekazywane organom uprawnionym na podstawie przepisów prawa oraz powierzone na podstawie umowy powierzenia oraz osobom upoważnionym do przetwarzania danych.

Powyższe informacje zrozumiałem i przyjąłem do wiadomości.

.....
(data i podpis Pracownika)

Załącznik nr 3
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Klauzula informacyjna
przekazywana wykonawcom wykonującym zadania na podstawie umów cywilno – prawnych

Zgodnie z treścią art. 13 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) dalej RODO – informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Zespół Parków Krajobrazowych Województwa Śląskiego w Katowicach z siedzibą w Będzinie, ul. I. Krasickiego 25, 42-500 Będzin.
2. Z Inspektorem Ochrony Danych można kontaktować się mailowo, pod adresem iod@zpk.com.pl lub pocztą tradycyjną pod adresem kontaktowy Administratora danych
3. Pani/Pana dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. b, c, f RODO, w celu związanym z zawarciem umowy cywilno - prawnej.
4. Pani/Pana dane osobowe będą przechowywane w trakcie okresu współpracy z Zespołem Parków Krajobrazowych Województwa Śląskiego oraz na potrzeby archiwizacji dokumentacji związanej ze współpracą według okresów wskazanych w przepisach szczegółowych.

5. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu.
6. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
7. Podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne dla celów związanych z nawiązaniem i przebiegiem współpracy.
8. Pani/Pana dane nie będą poddawane profilowaniu. Zespół Parków Krajobrazowych Województwa Śląskiego nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
9. Dane osobowe są przekazywane organom uprawnionym na podstawie przepisów prawa oraz powierzone na podstawie umowy powierzenia oraz osobom upoważnionym do przetwarzania danych.

Powyższe informacje zrozumiałem i przyjąłem do wiadomości.

.....

(data i podpis Wykonawcy)

Załącznik nr 4
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Klauzula informacyjna

przekazywana opiekunom dzieci uczestniczących we wszelkich formach edukacji ekologicznej

Zgodnie z treścią art. 13 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 RODO – informujemy, że: Administratorem Pani/Pana danych osobowych jest Zespół Parków Krajobrazowych Województwa Śląskiego w Katowicach z siedzibą w Będzinie, ul. I. Krasickiego 25, 42-500 Będzin.

1. Z Inspektorem Ochrony Danych można kontaktować się mailowo, pod adresem iod@zpk.com.pl lub pocztą tradycyjną pod adresem kontaktowy Administratora danych.
2. Dane osobowe osób uczestniczących we wszelkich formach edukacji ekologicznej ZPKWŚ przetwarzane w celach ewidencyjnych, sprawozdawczych, promocyjnych i informacyjnych na podstawie art. 6 ust. 1 lit. c, e ww. Rozporządzenia.
3. Dane osobowe są przekazywane organom uprawnionym na podstawie przepisów prawa oraz powierzone na podstawie umowy powierzenia oraz osobom upoważnionym do przetwarzania danych.

4. Dane osobowe będą przetwarzane przez okres 2 lat, a następnie archiwizowane zgodnie z Ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym, z późn. zmianami.
5. Osoby uczestniczące we wszelkich formach edukacji ekologicznej ZPKWŚ posiadają prawo do: dostępu do treści swoich danych i ich poprawiania, sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, wniesienia sprzeciwu, cofnięcia zgody na przetwarzanie.
6. Osoby uczestniczące we wszelkich formach edukacji ekologicznej ZPKWŚ mają prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych ich dotyczących naruszałoby przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 roku.
7. Pani/Pana dane nie będą poddawane profilowaniu. Zespół Parków Krajobrazowych Województwa Śląskiego nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
8. Podanie danych osobowych (imię i nazwisko uczestnika/opiekuna grupy, nazwa i adres placówki oświatowej) jest dobrowolne, aczkolwiek niezbędne do organizacji edukacji ekologicznej ZPKWŚ. Niepodanie danych osobowych może skutkować brakiem możliwości korzystania z wszelkich form edukacji ekologicznej ZPKWŚ.

Powyższe informacje zrozumiałem i przyjąłem do wiadomość

…… podpis opiekuna grupy

Zatwierdzam:

Załącznik nr 5
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia ……. r. w Będzinie, zwana dalej „Umową”,

pomiędzy:

Zespołem Parków Krajobrazowych Województwa Śląskiego,

ul. Ignacego Krasickiego 25, 42-500 Będzin, NIP: 954-277-00-64

zwanym w dalszej części umowy „**Zleceniodawcą”** lub **„Administratorem danych"**

reprezentowanym przez:

WZÓR

Hanna Pompa-Obońska – Dyrektor ZPKWŚ

a

…….
…….
……
zwaną w dalszej części umowy **„Zleceniobiorcą”** lub **„Podmiotem przetwarzającym”**

reprezentowaną przez:

1. ……

2. ……

§ 1

Powierzenie przetwarzania danych osobowych

1. Przedmiotem niniejszej umowy jest przetwarzanie danych osobowych przez Podmiot przetwarzający w imieniu i na polecenie Administratora danych.
2. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych, tj. 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 (zwanego w dalszej części „Rozporządzeniem", po rozpoczęciu stosowania) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
3. Administratorem danych w rozumieniu art. 4 ust. 7 Rozporządzenia jest Zleceniodawca.
4. Podmiotem przetwarzającym w rozumieniu art. 4 ust. 8 Rozporządzenia, któremu Zleceniodawca powierza przetwarzanie danych osobowych, jest Zleceniobiorca.
5. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
6. Zleceniobiorca oświadcza, iż dysponuje środkami umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Administratora danych, w zakresie i celu określonym w Umowie.
7. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.
8. Zleceniobiorca oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi określone w aktualnie obowiązujących przepisach prawa.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy (wskazać kategorię oraz rodzaj danych):
   1) ……
   2) ……
2. Powierzenie przetwarzania danych osobowych na mocy niniejszej Umowy następuje wyłącznie w celu i w zakresie realizacji Usługi.
3. Przetwarzanie powierzonych danych osobowych zwykłych i/lub wrażliwych odbywa się po stronie Zleceniobiorcy przy wykorzystaniu systemów informatycznych/dokumentacyjnych.

4. Zleceniobiorca zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją umowy i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.
5. Zleceniobiorca przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora danych.
6. Na wniosek Administratora danych lub osoby, której dane dotyczą, Zleceniobiorca wskaże miejsca, w których przetwarza powierzone dane.

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia. Środki te mają na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych. W szczególności Zleceniobiorca zobowiązany jest zabezpieczyć dane przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych, w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.
3. Do przetwarzania danych mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie, o którym mowa w art. 29 Rozporządzenia. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy, jak również zapewnia, iż osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz odpowiedzialnością za ich nieprzestrzeganie.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust. 3 pkt. b) Rozporządzenia) przetwarzanych danych i sposobów ich zabezpieczenia przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem w ciągu 30 dni zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa (prawo Unii lub prawo państwa członkowskiego – prawo polskie), nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie realizacji obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi, w ciągu 24 godzin po stwierdzeniu naruszenia.
8. Zgłoszenie, o którym mowa w ust. 7, następuje w formie pisemnej i zawiera co najmniej:
    1) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    2) imię i nazwisko oraz dane kontaktowe osoby, od której można uzyskać więcej informacji;
    3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
    4) opis środków zastosowanych lub proponowanych przez Procesora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

9. Podmiot przetwarzający zobowiązuje się do współpracy z Administratorem danych w zakresie obsługi zdarzenia i usunięcia jego skutków.

Zatwierdzam

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego (prawo polskie), któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania

Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w § 3 ust. 3 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot 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.
2. Zleceniobiorca odpowiada za szkody spowodowane przetwarzaniem danych osobowych, jeżeli nie dopełnił obowiązków określonych w niniejszej Umowie, lub gdy działał niezgodnie z instrukcjami Administratora danych albo wbrew tym instrukcjom.
3. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadomo, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu *Ochrony Danych Osobowych* (Organ nadzoru). Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia podpisania umowy, do momentu ……
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem jednomiesięcznego okresu wypowiedzenia.

§8

Rozwiązanie umowy

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z umową;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§9

Zasady zachowania poufności

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

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla siedziby Administratora danych.

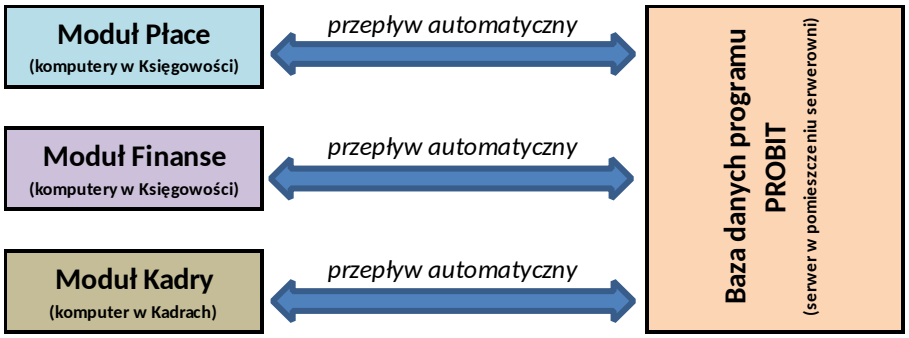
_____ _____

Administrator danych **Podmiot przetwarzający**

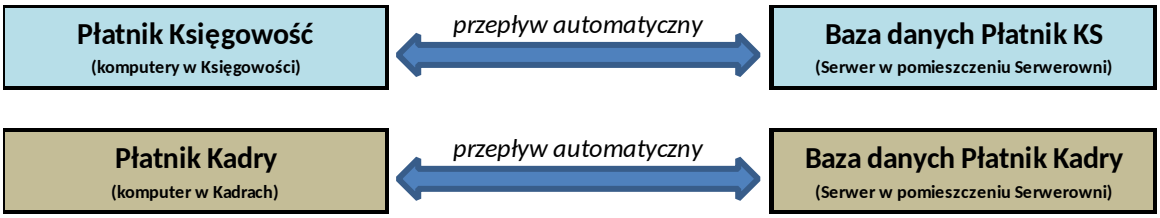
Załącznik nr 6
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Przepływ danych pomiędzy systemami

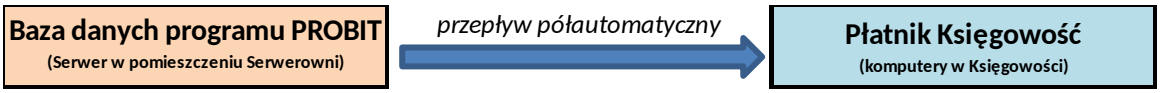
1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przesyłanie danych pomiędzy systemami może odbywać się w sposób półautomatyczny, poprzez ręczne pobranie pliku z jednego programu i przeniesienie go do drugiego z wykorzystaniem funkcji eksportu/importu (dane przesyłane są z serwera poprzez sieć lokalną) lub w sposób automatyczny (program automatycznie przesyła dane do bazy na serwerze poprzez sieć lokalną).
3. Dane osobowe przetwarzane w Zespole Parków Krajobrazowych Województwa Śląskiego za pomocą opisanego w Załączniku nr 2 oprogramowania przesyłane są w następujący sposób:
   a. Program Probit:



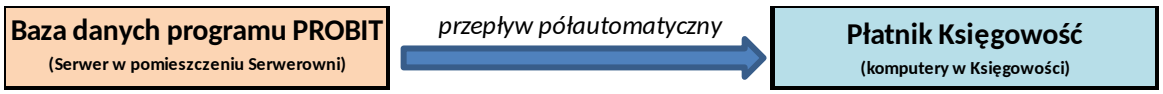
b. Program Płatnik:



c. Przepływ pomiędzy programami Probit i Płatnik:



d. Przepływ pomiędzy programem Probit i Bankowością Internetową



W przypadku pozostałych programów bezpośredni przepływ nie istnieje.

Załącznik nr 7
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Klauzula informacyjna

dotycząca monitoringu wizyjnego

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/670 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 96/46/WE (ogólne rozporządzenie o ochronie danych), zwanym dalej RODO informujemy, iż:

1. Administratorem Pani/Pana danych osobowych jest Zespół Parków Krajobrazowych Województwa Śląskiego w Katowicach z siedzibą w Będzinie, ul. I. Krasickiego 25, 42-500 Będzin.
2. Z Inspektorem Ochrony Danych można kontaktować się mailowo, pod adresem iod@zpk.com.pl lub pocztą tradycyjną pod adres kontaktowy Administratora danych.

3. Dane osobowe tj. wizerunek będzie przetwarzany w celu zapewnienia bezpieczeństwa ludzi i mienia zgodnie z art. 6 ust. 1 lit. c i f RODO.
4. **Podanie przez Pa**ństwa danych osobowych jest dobrowolne. Konsekwencją odmowy udostępnienia danych jest brak (pra[illegible]nia do przebywania na terenie ZPKWŚ.
5. **Dane osobowe b**ędą przechowywane przez okres maksymalnie 3 miesięcy lub do czasu prawomocnego zakończenia postępowania prowadzonego na podstawie prawa.
6. **Odbiorcami danych s**ą osoby upoważnione przez administratora, podmioty przetwarzające, z którymi Administrator zawarł odpowiednie umowy powierzenia oraz podmioty, których uprawnienia wynikają z przepisu prawa.
7. **Posiada Pani/Pan prawo do żądania dostępu od swoich danych osobowych, ich sprostowania oraz usunięcia, jak również do żądania ograniczenia przetwarzania czy wniesienia sprzeciwu. Pani/Pan ma prawo do cofnięcia zgody, w każdym momencie. Cofnięcie zgody nie będzie wpływać na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.**
8. **Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie Pani/Pana danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.**
9. **Pani/Pana dane osobowe nie będą podlegać zautomatyzowanym decyzjom, w tym profilowaniu.**
10. **Pani/Pana dane nie będą przekazywane do państwa trzeciego czy organizacji międzynarodowej.**

Powyższe informacje zrozumiałem i przyjąłem do wiadomości.

WZÓR

Zatwierdza

.....
(data i podpis)

Załącznik nr 8
Do Polityki Bezpieczeństwa Informacji w zakresie danych osobowych

Klauzula informacyjna

dla kandydata w procesie rekrutacji

1) Dane osobowe przetwarzane są zgodnie z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2019 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 (RODO) (z późn. zm.).
2) Każdy kandydat biorący udział w procesie rekrutacji podaje swoje dane dobrowolnie. Bez podania wymaganych danych osobowych udział w procesie rekrutacji nie będzie możliwy,
3) Administratorem Pana/Pani danych osobowych jest Zespół Parków Krajobrazowych Województwa Śląskiego w Katowicach z/s w Będzinie 42-500 Będzin, ul. Ignacego Krasickiego 25, reprezentowany przez Dyrektora ZPKWŚ.

4) We wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z ich przetwarzaniem należy kontaktować się elektronicznie z Inspektorem Ochrony Danych pod adresem iod@zpk.com.pl lub listownie pod dane kontaktowe Administratora.

5) Pana/Pani dane osobowe przetwarzane będą na potrzeby rekrutacji na stanowisko pracy w Zespole Parków Krajobrazowych Województwa Śląskiego w Katowicach z/s w Będzinie na podstawie art. 6 ust. 1 lit. a, b, c RODO.

6) Pana/Pani dane osobowe będą przechowywane przez czas niezbędny do przeprowadzenia procesu rekrutacji na stanowisko pracy w Zespole Parków Krajobrazowych Województwa Śląskiego w Katowicach z/s w Będzinie, a po zakończeniu procesu rekrutacji przez okres 3 miesięcy od dnia nawiązania stosunku pracy z osobą wyłonioną w drodze naboru. W tym okresie istnieje możliwość odbioru swoich dokumentów aplikacyjnych za pokwitowaniem, a nieodebrane
w ww. terminie dokumenty zostaną komisyjnie zniszczone.

7) Posiada Pan/Pani prawo dostępu do treści swoich danych, do ich sprostowania, usunięcia, ograniczenia przetwarzania a także do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do cofnięcia zgody na przetwarzanie danych osobowych, jeśli taka zgoda była konieczna do rozpoczęcia czynności przetwarzania.

8) Posiada Pan/Pani prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,

9) Podane przez Pana/Panią dane nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, nie będą też profilowane oraz nie będą przesyłane do państwa trzeciego czy organizacji międzynarodowej.

Powyższe informacje zrozumiałem i przyjąłem do wiadomości.

…… (data i podpis)

Załącznik nr 2
do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

§1
Postanowienia ogólne

1. Wprowadza się Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w systemach informatycznych zwaną dalej „instrukcją” na podstawie 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).
2. Instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

§2
Obszar przetwarzania danych

1. Wszystkie pomieszczenia, które należą do obszaru przetwarzania danych, wyposażone są w drzwi zamykane na klucz.
2. W czasie, gdy nie znajdują się w nich osoby upoważnione, pomieszczenia są zamykane w sposób uniemożliwiający wstęp osobom nieupoważnionym.
3. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych wyłącznie za zgodą Administratora Danych Osobowych lub w obecności osób upoważnionych.

§3
Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Zabezpieczenie infrastruktury przed skutkami awarii zasilania:
   w celu zabezpieczenia przed skutkami awarii zasilania krytyczne stanowiska (komputery stacjonarne w Dziale Księgowości, Kadr oraz Serwer) zostały wyposażone w urządzenia UPS, które w razie awarii sieci energetycznej umożliwiają zakończenie prac oraz bezpieczne zamknięcie systemu. Podtrzymanie napięcia trwa około 5 minut.
2. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem:
   1) komputery i programy służące do przetwarzania danych osobowych zabezpieczone zostały przed nieautoryzowanym uruchomieniem za pomocą uwierzytelnienia (identyfikatory użytkowników oraz hasła),
   2) w celu zabezpieczenia sprzętu przed instalacją nielegalnego oprogramowania każdy komputer jest zabezpieczony dwoma profilami:
      a) konto lokalne do którego dostęp posiada pracownik przetwarzające dane osobowe (brak możliwości instalowania oprogramowania, zmiany ustawień zabezpieczeń itp.),
      b) konto administratora do którego dostęp posiada Pomoc informatyczna.
   3) w celu zabezpieczenia dostępu do komputera osobom nieupoważnionym w czasie nieobecności pracownika upoważnionego, konta ustawione mają automatyczny wygaszacz ekranu, który załącza się po 5 minutach bezczynności, (wznowienie pracy wymaga uwierzytelnienia),
   4) komputery powinny być ustawione w ten sposób by osoby niepowołane nie miały do nich ułatwionego dostępu.
3. Zabezpieczenia sprzętowe i programowe przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych:
   1) wszystkie komputery służące do przetwarzania danych osobowych zabezpieczone zostały przez programy antywirusowe chroniące przed szkodliwym oprogramowaniem.
   2) urządzenie sieciowe klasy UTM, które łącznie z systemem bezprzewodowym (z wydzieloną strefą ogólnodostępną) chroni przed dostępem do sieci osób nieuprawionych.
4. Zabezpieczenie elektronicznych nośników informacji:

1) nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi;
2) w przypadku gdy wymienne nośniki informacji, są wynoszone poza obszar jednostki powinno to być realizowane zgodnie z zasadami pracy zdalnej.
3) użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania;
4) podlegające likwidacji uszkodzone lub przestarzałe nośniki, w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny.

§4
Rejestrowanie i wyrejestrowanie użytkownika

1. Użytkownikiem systemu informatycznego (osobą upoważnioną) może być:
   1) osoba upoważniona przez administratora danych osobowych do przetwarzania danych osobowych w ZPKWŚ, która posiada upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład,
   2) pracownik innego podmiotu lub przedsiębiorca będący osobą fizyczną prowadzącą działalność na podstawie wpisu do ewidencji działalności gospodarczej, który świadczy na podstawie umowy usługi związane z ich pracą w systemie informatycznym (serwis, zlecenie przetwarzania danych itp.).
2. Uzyskanie uprawnień następuje poprzez:
   1) założenie konta pracownika,
   2) nadanie określonych uprawnień do korzystania z systemu komputerowego.
3. Pisemny wniosek o zarejestrowanie użytkownika składa bezpośredni przełożony pracownika.
4. Wniosek zostaje przekazany do Inspektora Ochrony Danych, który może zgłosić sprzeciw wobec przyznania uprawnień, ze względu na zagrożenie naruszenia bezpieczeństwa danych osobowych.
5. W przypadku zakończenia pracy w Jednostce, stosuje się następującą procedurę wyrejestrowania użytkownika:
   1) na karcie obiegowej, na której osoba odchodząca zbiera podpisy potwierdzenia rozliczenia się z pracodawcą, znajduje się pozycja stwierdzająca fakt usunięcia lub zablokowania profilu użytkownika,
   2) wykonanie tej operacji jest jednoznaczne z uniemożliwieniem dostępu do systemu dla pracownika, z którym rozwiązano umowę o pracę w ZPKWŚ.

§5
Sposób przydziału haseł i zasady korzystania z nich

1. Każdorazowe uwierzytelnienie użytkownika w systemie następuje po podaniu przypisanego hasła do spersonalizowanego loginu.
2. Używanie hasła jest obowiązkowe dla każdego użytkownika, posiadającego login w systemie.
3. Uwierzytelnienia (identyfikatory użytkowników, administratorów i hasła) do programów służących do przetwarzania danych osobowych umieszczone są w kasie pancernej zabezpieczonej zamkiem w pomieszczeniu Księgowości.
4. W jednostce obowiązują następujące zasady korzystania z haseł:
   1) zabrania się ujawniania haseł jakimkolwiek osobom trzecim,

2) zabrania się zapisywania haseł lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim,
3) w przypadkach awaryjnych (np. nieobecność Pomocy informatycznej) hasło administratora, które znajduje się w szafie pancernej w Dziale Księgowym, może być przekazane osobie zastępującej za zgodą i wiedzą Inspektora Ochrony Danych. Fakt ten zostaje potwierdzony protokołem, który przechowuje Inspektor Ochrony Danych.

5. Pracownicy przetwarzający dane osobowe winni zmieniać hasło dostępu do systemu nie rzadziej niż raz na 60 dni.
6. Hasło powinno składać się z co najmniej 10 znaków (z dużych i małych liter, cyfr lub znaków specjalnych).
7. Hasło nie może być słownikowe, nie może zawierać imienia, nazwiska, miejscowości lub daty urodzenia
8. Prawidłowe wykonywanie obowiązków związanych z korzystaniem użytkowników z haseł nadzoruje Inspektor Ochrony Danych przy pomocy - Pomocy Informatycznej. Nadzór ten w szczególności polega na obserwacji funkcjonowania mechanizmu uwierzytelniania i przywracania stanu prawidłowego w przypadku nieprawidłowości.

§6
Rozpoczęcie i zakończenie pracy

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie zawiadamia Inspektora Ochrony Danych.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   1) włączenie komputera,
   2) uwierzytelnienie się (zalogowanie w systemie) za pomocą hasła do przypisanego loginu.
3. Niedopuszczalne jest uwierzytelnianie się na hasło i login innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.
4. Zakończenie pracy użytkownika w systemie następuje po „wylogowaniu się" z systemu.
5. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności urządzenia przenośne, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
6. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest „wylogować się" lub zaktywizować wygaszacz ekranu z opcją ponownego „logowania" się do systemu.
7. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania, użytkownik niezwłocznie powiadamia o nich Pomocy Informatycznej.

§7
Tworzenie, przechowywanie i likwidacja kopii zapasowych

1. Kopie zapasowe są tworzone, przechowywane i wykorzystywane z uwzględnieniem następujących zasad:
   1) codzienne kopie zapasowe (całościowe) oprogramowania PROBIT, PŁATNIK oraz plików z działu Księgowości i Kadr przechowywanych na serwerze – są wykonywane

w sposób zautomatyzowany. Zapisywane są na serwerze głównym. Likwidacja tych kopii zapasowych następuje po tygodniu poprzez trwałe ich usunięcie,

2) comiesięczne kopie zapasowe (całościowe) programów służących do przetwarzania danych osobowych są wykonywane przez Pomoc Informatyczną i przechowywane na zew, nośniku danych. Kopie zapasowe przechowywane są w sejfie zamykanym na klucz/ kod. Likwidacja tych kopii zapasowych następuje po 6 miesiącach poprzez ich trwałe usunięcie.

§8

Sprawdzanie komputerów pod względem obecności wirusów

1. Sprawdzanie obecności wirusów komputerowych dokonywane jest poprzez zainstalowane oprogramowanie antywirusowe, które skanuje automatycznie, bez udziału użytkownika, na obecność wirusów wszystkie pliki. Program jest zainstalowany na wszystkich stacjach roboczych.
2. Program antywirusowy w sposób automatyczny skanuje elektroniczne nośniki informacji oraz skrzynkę pocztową przychodzącą.
3. Aktualizacje oprogramowania dokonywane są w sposób automatyczny (sprawdzanie dostępności aktualizacji co 1 godzinę).
4. Po każdej naprawie i konserwacji komputera należy dokonać sprawdzenia poprawności działania programu antywirusowego, w razie konieczności zainstalować ponownie program antywirusowy.
5. W przypadku stwierdzenia obecności złośliwego oprogramowania lub jakichkolwiek nieprawidłowości w działaniu oprogramowania antywirusowego, należy bezzwłocznie zgłosić ten fakt do Pomocy Informatycznej.

§9

Zasady przeglądów i konserwacji infrastruktury informatycznej służącego do przetwarzania danych osobowych

1. Przeglądu i konserwacji infrastruktury informatycznej dokonuje Pomoc Informatyczna.
2. W przypadku konieczności przekazania urządzeń, dysków lub innych nośników zawierających dane osobowe podmiotowi zewnętrznemu do przetwarzania danych osobowych np. na wypadek prac serwisowych lub naprawczych, ustalona została następująca zasada:
   nośniki wymontowuje się i pozostawia zabezpieczone u Pomoc Informatycznej, lub nośniki informacji pozbawia się wcześniejszego zapisu w sposób uniemożliwiający ich odzyskanie przez osoby nieupoważnione. Preferowaną formą realizacji prac serwisowych i naprawczych jest wykonywanie ich pod nadzorem Pomoc Informatycznej na terenie ZPKWŚ, lub w sytuacjach koniecznych – poza nią. Wymagany jest pisemny protokół z zakresu wykonanych prac wraz z klauzulą poufności, który każdorazowo stworzy Administrator Systemów Informatycznych.

§10

Komunikacja w sieci komputerowej

1. W zakresie korzystania z sieci komputerowej w ZPKWŚ obowiązują następujące zasady:
   1) zabrania się instalacji przez pracowników jakiegokolwiek oprogramowania,

2) oprogramowanie na komputerach może być zainstalowane wyłącznie przez Pomoc Informatyczną,
3) zabrania się przekazywania za pośrednictwem sieci telekomunikacyjnej do stron trzecich jakichkolwiek danych osobowych stanowiących własność ZPKWŚ, chyba że zgodę na takie rozwiązanie wyraził Inspektor Ochrony Danych,
4) zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek nielegalnych programów oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za zgodą Pomocy Informatycznej i tylko w uzasadnionych przypadkach,
5) pracownicy zobowiązani są do korzystania z Internetu wyłącznie w celach służbowych,
6) nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł,
7) w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka – certyfikat wystawiony dla strony) oraz adresu www. rozpoczynającego się frazą „https:". Wszyscy pracownicy ZPKWŚ są zobowiązani do zachowania szczególnej ostrożności przy korzystaniu
z przeglądarek internetowych.
8) dodatkowo należy:
   a) weryfikować autentyczności strony: Zawsze należy sprawdzić, czy adres URL strony jest poprawny i nie zawiera literówek, które mogą wskazywać na próbę oszustwa,
   b) aktualizować przeglądarki i oprogramowania antywirusowego: Upewnij się, że przeglądarka internetowa oraz programy antywirusowe są zawsze zaktualizowane, co pomoże chronić przed najnowszymi zagrożeniami,
   c) unikać publicznych sieci Wi-Fi: Publiczne sieci Wi-Fi mogą być łatwo celem ataków, które przechwytują dane przesyłane między użytkownikiem a stroną internetową, nawet jeśli połączenie jest szyfrowane,
   d) przyglądać się certyfikatom SSL: Warto sprawdzać, kto wydał certyfikat SSL oraz czy jest on ważny. Niektóre przeglądarki oferują opcje, które pozwalają na szybkie sprawdzenie szczegółów certyfikatu,
   e) wprowadzić dwuskładnikowe uwierzytelnianie (2FA): Gdy to możliwe, należy korzystać z dwuskładnikowego uwierzytelniania, co zapewnia dodatkową warstwę bezpieczeństwa nawet w przypadku, gdy strona jest bezpieczna.

§11
Procedura korzystania z poczty elektronicznej

1. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza jednostkę należy wykorzystywać mechanizmy kryptograficzne (szyfrowanie wewnętrznych plików). Hasło takie musi składać się z minimum 8 znaków (duże i małe litery, cyfry lub znaki specjalne i należy je przesłać inną metodą niż mail np. podać telefonicznie lub poprzez wiadomość SMS.
2. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

3. Zaleca się, aby użytkownik podczas przesyłania danych osobowych poprzez wiadomość e-mail zawarł w treści prośbę o potwierdzenie otrzymania i przeczytania wiadomości przez adresata.

Załącznik nr 3
do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Analiza ryzyka i skutków przy przetwarzaniu danych osobowych

Rozdział 1
CEL

Administrator Danych Osobowych w celu podjęcia ustaleń w zakresie obszarów zagrożeń, które wymagają zabezpieczenia w związku
z przetwarzaniem danych osobowych winien przeprowadzić analizę ryzyka, której efektem winno być wskazanie obszarów, w których owe ryzyko wykracza poza akceptowalne granice i generuje istotne prawdopodobieństwo powstania naruszeń bezpieczeństwa danych osobowych oraz naruszeń praw i wolności osób powstałych w związku z przetwarzaniem ich danych osobowych.

Efektem analizy winno być wypracowanie adekwatnych zabezpieczeń, które prowadzą do minimalizacji ryzyka wysokiego do granic dopuszczalnej akceptacji. Zastosowanie wszystkich wskazanych grup zabezpieczeń winno prowadzić do eliminacji lub obniżenia do granic akceptacji wszystkich wysokich ryzyk powstania naruszeń bezpieczeństwa danych osobowych.

Analiza ryzyka jest elementem koniecznym dla skutecznego wdrożenia i funkcjonowania systemu ochrony danych osobowych i winna być realizowana przed przystąpieniem do czynności przetwarzania, po każdej istotnej zmianie procesu przetwarzania oraz okresowo, celem oceny adekwatności stosowanych zabezpieczeń.

Rozdział 2
ZAKRES STOSOWANIA

Procedurę stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych jak i wykonujących czynności na podstawie odrębnych umów.

Rozdział 3
TRYB POSTĘPOWANIA

§ 1
Rola analizy ryzyka w ochronie danych osobowych

Przepisy prawa nakładają na Administratora Danych Osobowych obowiązki i odpowiedzialność prawną za przetwarzanie danych osobowych prowadzone przez niego samego lub w jego imieniu. W szczególności Administrator Danych Osobowych ma obowiązek wdrożenia odpowiednich i skutecznych środków ochrony w postaci zabezpieczeń organizacyjnych i technicznych. Ponadto powinien on być w stanie wykazać, że czynności przetwarzania prowadzone są w zgodzie z wymogami rozporządzenia ogólnego o ochronie danych osobowych, a dobrane i zaimplementowane środki ochrony uwzględniają charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

§ 2
Metodologia analizy ryzyka

Metodologia oparta została o przeprowadzenie analizy zagrożeń dla celów bezpieczeństwa informacji wynikających z normy ISO 27001 w odniesieniu i przy uwzględnieniu specyfiki przetwarzania danych osobowych dla zagrożeń bezpieczeństwa informacji uwzględnionych w zapisach normy przy uwzględnieniu kontekstu organizacji. W kolejnych krokach szacowane jest prawdopodobieństwo materializacji zagrożenia oraz skutek, jaki dla osoby, której dane dotyczą może przynieść, których celem jest oszacowanie ryzyka pierwotnego. Następnie dokonuje się korekty prawdopodobieństwa w oparciu o zabezpieczenia, co prowadzi do oszacowania ryzyka rezydualnego.

§ 3
Ocena prawdopodobieństwa i skutku

Ryzyko prawdopodobieństwa wystąpienia naruszeń bezpieczeństwa danych osobowych w związku z brakiem realizacji celów bezpieczeństwa ustalane jest w oparciu o szacowane wartości prawdopodobieństwa wystąpienia zagrożenia oraz skutku, jaki może przynieść dla osoby, której dane przetwarzamy. Prawdopodobieństwo, jak i skutek estymujemy na skali 1-5, gdzie:

Prawdopodobieństwo na poziomie:

5 - oznacza bardzo wysoką szansę (niemalże pewność) wystąpienia zdarzenia, gdy nie zostanie ono zabezpieczone

4 – oznacza wysoką szansę wystąpienia zdarzenia

3 – oznacza średnią szanse wystąpienia zdarzenia

2 – oznacza niską szansę wystąpienia zdarzenia

1- oznacza pomijalną (śladową) szansę wystąpienia zdarzenia

Skutek, oznacza w przypadku materializacji zagrożenia:

5 – możliwy bardzo dotkliwy skutek dla osoby, której dane przetwarzamy w związku z naruszeniem przepisów prawa, powstaniem poważnych strat finansowy lub utratą reputacji

4 - możliwy znaczący skutek dla osoby, której dane przetwarzamy w związku z naruszeniem przepisów prawa, powstaniem poważnych strat finansowy lub utratą reputacji

3 - ograniczony skutek dla osoby, której dane przetwarzamy w związku powstaniem strat finansowych lub utratą reputacji

2 - ograniczony skutek dla osoby, której dane przetwarzamy w związku powstaniem strat finansowych lub utratą reputacji

1 – znikomy skutek dla osoby, której dane przetwarzamy w związku powstaniem strat finansowych lub utratą reputacji

Estymacja ryzyka pierwotnego

Ryzyko pierwotne wyliczane jest jako znormalizowany iloczyn prawdopodobieństwa wystąpienia zagrożenia oraz istotności skutku jaki dla osoby, której dane przetwarzane są przez ZPKWS. Ryzyko pierwotne wyliczane jest w przypadku braku zabezpieczeń. Szacowane ryzyko pierwotne normalizowane jest do skali 1-5 wg wzoru:

$$R=\sqrt{P*S}$$

gdzie:

R – szacowane ryzyko pierwotne

P – prawdopodobieństwo wystąpienia

S – skutek dla organizacji

Natomiast otrzymane wartości **ryzyka pierwotnego** oznaczają odpowiednio:

5 – oznacza wysokie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku braku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

4 – oznacza średnio wysokie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku braku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

3 – oznacza średnie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku braku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

2 – oznacza niskie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku braku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

1 – oznacza pomijalne (śladowe) ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku braku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

Korekta prawdopodobieństwa

Korekta prawdopodobieństwa pozwala na oszacowanie **ryzyka rezydualnego** w oparciu o potwierdzenie stosowania zabezpieczeń.

Otrzymane wartości **ryzyka rezydualnego** oznaczają odpowiednio:

5 – oznacza wysokie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

4 – oznacza średnio wysokie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

3 – oznacza średnie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

2 – oznacza niskie ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń.

1 – oznacza pomijalne (śladowe) ryzyko wystąpienia naruszenia bezpieczeństwa danych osobowych w przypadku skutecznego zabezpieczenia danego zagrożenia / grupy zagrożeń

§ 4
Postępowanie z ryzykiem rezydualnym

Na potrzeby prowadzonej analizy, przyjęto założenie, że obszary ryzyka wysokie (5) zawsze wykraczają poza granice możliwej akceptacji i wymagają bezwzględnego zabezpieczenia poprzez adekwatny zestaw środków organizacyjnych i technicznych. Ponadto zaleca się, aby obszary, w których ryzyko oceniono, jako średnio wysokie (4) oraz średnie (3), zostały zabezpieczone poprzez zastosowanie adekwatnych środków organizacyjnych i technicznych, chyba, że Administrator Danych Osobowych podejmie decyzje o akceptacji ryzyka w danym obszarze na poziomie średnim. Ryzyko na poziomie niskim (2) oraz pomijalne (1) stanowią poziomy akceptowalne. Dodatkowo zaakceptowane ryzyka na poziomie średnio wysokim (4) i średnim (3) powinny być monitorowane.

Pozostawienie niezabezpieczonych ryzyk na poziomie wysokim wymaga przeprowadzenia oceny skutków przetwarzania w odniesieniu do każdej czynności przetwarzania.

W przypadku identyfikacji na etapie oceny skutków wysokiego ryzyka naruszenia bezpieczeństwa danych osobowych przy braku zastosowania zabezpieczeń dla danego obszaru lub utrzymania wysokiego ryzyka rezydualnego (po zastosowaniu zabezpieczeń) niezbędne będzie wówczas przeprowadzenie konsultacji w w/w zakresie z organem nadzorczym.

Każda komórka organizacyjna przeprowadza cząstkową analizę ryzyka w procesach, w których uczestniczy. Następnie jej wyniki przekazywane są do Administratora Danych Osobowych, który w porozumieniu z Inspektorem Ochrony Danych dokona analizy wyników i podejmie ewentualne działania naprawcze.

Ocena ryzyka jest przeprowadzana w arkuszu kalkulacyjnym „Analiza ryzyka". Wzór arkusza zawiera załącznik nr 1 do niniejszej procedury.

§ 5
Załącznik nr 1

Wzór arkusza analizy ryzyka.

Analiza ryzyka .xls (na linku prawy przycisk myszy i wybierz „otwórz hiperlink)

Załącznik nr 4
do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Procedura postępowania z incydentami i naruszeniami ochrony danych osobowych

Rozdział 1
CEL

Celem procedury jest:

1) minimalizacja skutków wystąpienia incydentów i naruszeń bezpieczeństwa,
2) ograniczenie ryzyka występowania incydentów i naruszeń w przyszłości,
3) prawidłowe reagowanie osób upoważnionych do przetwarzania danych osobowych oraz osób upoważnionych do przebywania w obszarze przetwarzania danych osobowych w przypadku stwierdzenia incydentu lub naruszenia ochrony danych osobowych,
4) zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu oraz osobom, których dane dotyczą.

Rozdział 2
ZAKRES STOSOWANIA

Procedurę stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych jak i wykonujących czynności na podstawie odrębnych umów.

Rozdział 3
TRYB POSTĘPOWANIA

1. Procedura definiuje katalog incydentów i naruszeń zagrażających bezpieczeństwu danych osobowych, jednakże nie jest on zamknięty, oraz opisuje sposób reagowania na nie.
2. Incydent to możliwość wystąpienia ujawnienia, utraty lub niedostępności danych. Jest to sytuacja, która może prowadzić do naruszenia, czyli potwierdzonego już ujawnienia, utraty lub niedostępności danych.
3. Odpowiedzialność za prawidłowe zgłaszanie incydentów dotyczących bezpieczeństwa danych osobowych spoczywa na osobach upoważnionych oraz osobach upoważnionych do przebywania w obszarze przetwarzania danych osobowych dokonujących zgłoszeń.
4. Przełożony, Służba Informatyczna oraz Inspektor Ochrony Danych współpracują ze sobą po zgłoszeniu incydentu lub naruszenia bezpieczeństwa i odpowiedzialni są za:
   1) niezwłoczne reagowanie na incydenty lub naruszenia bezpieczeństwa danych osobowych w określony i z góry ustalony sposób,
   2) ocenę istniejących i potencjalnych incydentów lub naruszeń w zakresie bezpieczeństwa danych osobowych,
   3) ocenę przyczyn i skutków incydentów oraz naruszeń bezpieczeństwa danych osobowych w tym gromadzenie materiału dowodowego,

4) przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem.

5. Administrator Danych Osobowych odpowiedzialny jest za:
   1) ocenę wymagalności zgłoszenia naruszenia bezpieczeństwa danych osobowych do organu nadzorczego oraz osób, których dane dotyczą, po konsultacji z Inspektorem Ochrony Danych i/lub Służby Informatycznej (jeśli naruszenie dotyczy systemu informatycznego),
   2) przygotowanie treści zgłoszenia dotyczącego naruszenia bezpieczeństwa danych osobowych do organu nadzorczego oraz osób, których dane dotyczą we współpracy z Inspektorem Ochrony Danych,
   3) nadzór nad wprowadzaniem działań korygujących i naprawczych.
6. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się bądź wybite okna, itp.) nie powodujące utraty, ujawnienia, niedostępności danych,
   2) utrata usługi, urządzenia lub funkcjonalności nie powodująca utraty, ujawnienia, niedostępności danych,
   3) nieautoryzowana modyfikacja nie powodująca utraty, ujawnienia, niedostępności danych,
   4) pożar, zalanie nie powodujące utraty, ujawnienia, niedostępności danych,
   5) pozyskiwanie oprogramowania z nielegalnych źródeł,
   6) pojawianie się nietypowych komunikatów na ekranie,
   7) niemożność zalogowania się do systemu teleinformatycznego,
   8) spowolnienie pracy oprogramowania,
   9) niestabilna praca systemu teleinformatycznego,
   10) brak reakcji systemu na działania użytkownika,
   11) ponowny start lub zawieszanie się komputera,
   12) ograniczenie funkcjonalności oprogramowania.
7. Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:
   1) nieupoważniony dostęp, modyfikacje, kopiowanie, udostępnienie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie teleinformatycznym, jak i na nośnikach papierowych i elektronicznych,
   2) udostępnianie danych osobowych nieuprawnionym podmiotom,
   3) nieautoryzowany dostęp do danych osobowych przez połączenie sieciowe,
   4) niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych osobowych (np. pozostawienie kopii danych osobowych, nie zablokowanie dostępu do systemu, pozostawienie dokumentów z danymi osobowymi w miejscu dostępnym dla osób nieuprawnionych, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się dane osobowe),
   5) stworzenie niezabezpieczonego kanału dystrybucji danych osobowych,
   6) nielegalne bądź nieświadome ujawnienie danych osobowych,
   7) niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego,
   8) ujawnienie indywidualnych haseł dostępu do danych osobowych w systemie,
   9) przesyłanie danych osobowych przez Internet bez zabezpieczenia,

10) przesyłanie dokumentów papierowych i nośników elektronicznych z danymi osobowymi bez zabezpieczenia osobom nieuprawnionym,
11) wykonanie nieuprawnionych kopii danych osobowych,
12) kradzież nośników zawierających dane osobowe lub oprogramowanie,
13) kradzież sprzętu służącego do przetwarzania danych osobowych,
14) spowodowanie utraty danych osobowych w systemie teleinformatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
15) dopuszczenie do braku aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii,
16) niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt;
17) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe,
18) dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień,
19) brak szkoleń pracowników w zakresie zasad bezpieczeństwa danych osobowych,
20) pożar, zalanie powodujące utratę, ujawnienie lub niedostępność danych,
21) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych.

8. Osoby upoważnione, osoby upoważnione do przebywania w obszarze przetwarzania danych osobowych oraz podmioty przetwarzające mają obowiązek zgłaszania wszystkich incydentów i naruszeń dotyczących ochrony danych osobowych.
9. Przełożonego, Służbę Informatyczną oraz Inspektora Ochrony Danych powiadamia się telefonicznie, mailowo lub osobiście o zaistniałym incydencie lub naruszeniu. Każde zgłoszenie jest rejestrowane w formie elektronicznej.
10. Na stanowisku, na którym stwierdzono naruszenie bezpieczeństwa danych osobowych Przełożony, Służba Informatyczna lub Inspektor Ochrony Danych przejmują nadzór nad pracą na zagrożonym stanowisku pracy, odsuwając jednocześnie od stanowiska osobę, która dotychczas na nim pracowała, aż do czasu wydania odmiennej decyzji.
11. Wszelkie działania związane z samodzielnym naprawianiem, potwierdzaniem lub testowaniem potencjalnych słabości systemu są zabronione.
12. Dokonywanie zmian w miejscu incydentu lub naruszenia ochrony danych osobowych bez wiedzy i zgody Przełożonego, Służby Informatycznej lub Inspektora Ochrony Danych (w zależności od rodzaju naruszenia), jest dopuszczalne jedynie w sytuacji, gdy zachodzi konieczność ratowania życia lub zdrowia osób oraz mienia w przypadku ich bezpośredniego zagrożenia.
13. Przełożony, Służba Informatyczna oraz Inspektor Ochrony Danych przy wspólnej współpracy podejmują działania niezwłocznie po zgłoszeniu incydentu lub naruszenia. Zobowiązani są oni do przeprowadzenia postępowania wyjaśniającego w toku, którego:
    1) ustalają zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
    2) inicjują ewentualne działania dyscyplinarne,
    3) rekomendują działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.
14. W toku prowadzonego postępowania wyjaśniającego można udokumentować okoliczności naruszenia poprzez:
    1) sporządzenie notatki z przeprowadzonych oględzin miejsca zdarzenia,
    2) sporządzenie kopii obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem,

3) sporządzenie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń sytemu,
4) odebranie pisemnych wyjaśnień od osoby, która ujawniła naruszenie.

15. Inspektor Ochrony Danych wraz z Służbą Informatyczną oraz Przełożonym sporządza raport/notatkę, który zawiera, co najmniej następujące informacje: numer raportu, datę naruszenia, godzinę naruszenia, dane osoby zgłaszającej, dane IOD, okoliczności naruszenia, konsekwencje naruszenia, środki zastosowane, środki proponowane, informację czy został powiadomiony organu nadzorczy wraz z uzasadnieniem oraz informację czy zostały powiadomione osoby, których dane dotyczą wraz z uzasadnieniem, który rejestrowany jest w ewidencji naruszeń.
16. Ewidencja naruszeń powinna zawierać, co najmniej następujące informacje: numer raportu, data naruszenia, godzina naruszenia, dane osoby zgłaszającej, okoliczności naruszenia, zastosowane środki zaradcze, informację czy został powiadomiony organ nadzorczy wraz z uzasadnieniem oraz informację czy zostały powiadomione osoby, których dane dotyczą wraz z uzasadnieniem.
17. Na podstawie przeprowadzonego postępowania wyjaśniającego oraz zebranych dowodów i po konsultacji z Inspektorem Ochrony Danych, Administrator Danych Osobowych dokonuje oceny istotności incydentu oraz wymagalności zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego.
18. W przypadku istotnych incydentów, a przede wszystkim incydentów, które mogą powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą, Administrator Danych Osobowych w porozumieniu z Inspektorem Ochrony Danych tworzy plan działań mających na celu ograniczenie możliwości powstania incydentów podobnego typu w przyszłości.
19. W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu, Inspektor Ochrony Danych przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym Administratorowi Danych Osobowych celem ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.
20. Przy ocenie wymagalności zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego, Administrator Danych Osobowych wraz z Inspektorem Ochrony Danych biorą pod uwagę następujące skutki przetwarzania danych, które mogą powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą:
    1) kradzież tożsamości,
    2) straty finansowe,
    3) naruszenie dobrego imienia,
    4) naruszenie poufności danych chronionych tajemnicą zawodową,
    5) utrata przysługujących osobom praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
    6) ujawnienie szczególnych kategorii danych.
21. Naruszenia ochrony danych osobowych podlegają zgłoszeniu organowi nadzorczemu.
22. Zgłoszeń naruszeń do organu nadzorczego dokonuje Administrator Danych Osobowych bez zbędnej zwłoki, lecz nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
23. W przypadku braku zgłoszenia naruszenia w terminie do 72 godzin, Administrator Danych Osobowych zobowiązany jest dołączyć do zgłoszenia wyjaśnienia dotyczące przyczyny opóźnienia.
24. Zgłoszenie do organu nadzorczego obejmuje:

1) opis charakteru naruszenia ochrony danych osobowych, w tym wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
2) imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych, od którego można uzyskać więcej informacji,
3) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
4) opis środków zastosowanych lub proponowanych przez Administratora Danych Osobowych w celu zaradzenia naruszenia ochrony danych osobowych.

25. W przypadku, jeżeli nie da się udzielić informacji wymaganych w zgłoszeniu w tym samym czasie, należy je udzielać sukcesywnie bez zbędnej zwłoki.
26. Administrator Danych Osobowych nie będzie zobligowany do powiadomienia organu nadzorczego, jeżeli wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zastosował do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.
27. Jeżeli naruszenie bezpieczeństwa danych osobowych będzie mogło powodować wysokie ryzyko naruszenia praw i wolności osób, Administrator Danych Osobowych zobligowany jest poinformować o naruszeniu danych osoby, których dane dotyczą.
28. Powiadomienie o naruszeniu należy dokonać bez zbędnej zwłoki, jasnym, prostym językiem.
29. Administrator Danych Osobowych nie będzie zobligowany do powiadomienia osób, których dane dotyczą, jeżeli wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zastosował do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

Załącznik nr 1
do Procedury postępowania w przypadku naruszenia ochrony danych osobowych

Formularz rejestracji incydentu

WZÓR

Lp.	Okoliczności naruszenia	Charakter naruszenia	Ilość osób dotkniętych incydentem	Skutki naruszenia / incydentu	Data zdarzenia	Data rozpoczęcia wdrażania działań	Data zakończenia wdrażania działań	Osoba odpowiedzialna za wdrożenie działań

Zatwierdzam

:

Załącznik nr 5
do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Zasada zachowania poufności i ochrony danych osobowych

§ 1
Obowiązek osób dopuszczonych do przetwarzania danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach,
    b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę zarówno w trakcie trwania współpracy jak i po jej zakończeniu,
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę,
    d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
    e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego Zarządzenia lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności stanowiący odpowiedni **Załącznik nr 1 lub 2** do **Zasady zachowania poufności i ochrony danych osobowych**.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.

Załącznik nr 1
do Zasady zachowania poufności i ochrony danych osobowych

Wzór oświadczenia o poufności i potwierdzenia udziału w szkoleniu- ogólne

…… ……
(imię i nazwisko) *(miejscowość, data)*

WZÓR

OŚWIADCZENIE O POUFNOŚCI I POTWIERDZENIA UDZIAŁU W SZKOLENIU

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności z zapisami 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), POLITYKAMI WEWNĘTRZNYMI WPROWADZONYMI W Zarządzeniu nr 3/21 oraz zapisami „Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora zarówno w trakcie współpracy jak i po jej zakończeniu
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem poprzez stosowanie środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
- Zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

Zatwierdzam

……
podpis oświadczającego

Załącznik nr 2
do Zasady zachowania poufności i ochrony danych osobowych

Wzór oświadczenia o poufności – konserwatorzy, osoby sprzątające

……
……
(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności zapisami 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) politykami wewnętrznymi wprowadzonymi w Zarządzeniu nr 3/21 oraz zapisami "Regulaminu Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:

- zachowania w tajemnicy danych osobowych w sytuacji dostępu do nich podczas wykonywania czynności zleconych *) zarówno w trakcie trwania współpracy jak i po jej zakończeniu
- zabezpieczenia tych danych przed dostępem osób nieupoważnionych a następnie przekazanie ich do dyspozycji osób upoważnionych
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

……
podpis oświadczającego

*) *za czynności zlecone w obszarze przetwarzania danych osobowych rozumie się*

w szczególności: sprzątanie pomieszczeń, ochrona obiektów i pomieszczeń, konserwacja infrastruktury znajdującej się w obszarze przetwarzania danych osobowych

Załącznik nr 6
do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Ewidencja osób upoważnionych do przetwarzania danych osobowych

L.p.	Imię i Nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Stanowisko	Login/Identyfikator w systemie informatycznym	Uwagi
1.							
2.							
3.							
4.							
5.							
6.							
…							

Zatwierdzam

:

Załącznik nr 7

do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Rejestr czynności przetwarzania

Podstawa prawna: art. 30 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) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE Nr 119)

Administrator Danych Osobowych - **Zespół Parków Krajobrazowych Województwa Śląskiego reprezentowany przez Dyrektora ZPKWŚ**
……

WZÓR

Inspektor Ochrony Danych - **……**

Nazwa zbioru	Nazwa czynności przetwarzania	Komórka dokonująca czynności (Dział /Oddział)	**Cel przetwarzania danych**	**Kategorie osób, których dane dotyczą**	**Kategorie danych osobowych (zwykłe, wrażliwe, wyroki)**	Zakres przetwarzanych danych osobowych (pola informacyjne)	**Planowane terminy usunięcia danych**	Nazwa i dane podmiotu przetwarzającego oraz informacje o umowach powierzenia	**Nazwa współadministra i jego danych kontaktowych (jeśli dotyczy)**	**Kategorie odbiorców, którym dane zostały lub zostaną ujawnione**	Źródło zbierania danych	***Podstawa prawna przetwarzania danych***	Sposób przetwarzania tradycyjny/zautomatyzowany – programy służące do przetwarzania	**Ogólny opis tech i org. Środków bezpieczeństwa zastosowanych do ochrony danych**	**Transfer do kraju trzeciego lub organizacji międzynarodowej**	**Dokumentacja odpowiednich zabezpieczeń w przypadku transferu**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
	Bazy danych informatycznych															
	Bazy danych manualnych															

WZÓR

Sporządził:

…….

(data i podpis)

Zatwierdził:

……

(Data i podpis Administratora Danych Osobowych)

Zatwierdzam:

Załącznik nr 8

do Zarządzenia Dyrektora nr 5/25
z dnia 18.02.2025r.

Rejestr umów powierzenia przetwarzania danych osobowych

WZÓR

L.p.	Numer Umowy	Podmiot przetwarzający dane	Osoba zlecająca przetwarzanie danych	Data podpisania Umowy	Data zakończenia Umowy	Uwagi
1.						
2.						
3.						
4.						
5.						
6.						
…						

Zatwierdzam

: