Polityka Ochrony Danych Osobowych

w

PPHU An-Sat Katarzyna Łakoma z siedzibą w Paczkowie

(48-370 Paczków, ul. Wojska Polskiego 36)

dokument według stanu na sierpień 2020

I. POLITYKA OCHRONY DANYCH

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

Polityka zawiera:

1. Opis zasad ochrony danych obowiązujących w PPHU An-Sat Katarzyna Łakoma z siedzibą w Paczkowie przy ul. Wojska Polskiego 36 (dalej jako AnSat).
2. Odwołania do procedur, regulaminów lub instrukcji dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach wewnętrznych. Dokumenty wewnętrzne stają się obowiązujące z chwilą zatwierdzenia przez Administratora. Należy z nimi zapoznać każdą osobę upoważnioną do przetwarzania danych.

2 DEKLARACJA ZGODNOŚCI

AnSat zapewnia zgodność przetwarzania danych osobowych z regulacjami RODO oraz krajowymi przepisami dotyczącymi ochrony danych osobowych.

Organem działającym w imieniu Administratora w AnSat jest właściciel firmy – Katarzyna Łakoma, która zapewnia wdrożenie i przestrzeganie niniejszej Polityki oraz wewnętrznych procedur, regulaminów lub instrukcji dotyczących poszczególnych obszarów z zakresu ochrony danych osobowych.

Za nadzór i monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych Osobowych a za stosowanie Polityki odpowiedzialni są wszyscy pracownicy oraz członkowie personelu AnSat.

3 DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

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

Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"), możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

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

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

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

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

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

4 PODSTAWY OCHRONY DANYCH OSOBOWYCH

1. **Legalność** – AnSat dba o ochronę prywatności i przetwarza dane zgodnie z prawem, czyli zapewnia że spełniona jest przesłanka legalizującą to przetwarzanie.
2. **Bezpieczeństwo** – AnSat zapewnia odpowiedni poziom zabezpieczenia procesów przetwarzania danych poprzez wdrażanie rozwiązań organizacyjnych i technicznych oraz monitorowanie ich skuteczności.
3. **Prawa osób** – AnSat umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4. **Rozliczalność** – AnSat dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność przetwarzania z obowiązującymi przepisami.

5 ZASADY OCHRONY DANYCH

1. AnSat wypełniając obowiązki prawne, w szczególności wynikające z :
   ustawy z dnia 16 lipca 2004 Prawo telekomunikacyjne (Dz. U. 2004 Nr 171 poz. 1800 z późn. zm.)

   deklaruje, że dane są przetwarzane:
   1) w oparciu o podstawę prawną i zgodnie **z prawem** (legalizm na podstawie art. 6, 9 RODO),
   2) rzetelnie i uczciwie (**rzetelność**),
   3) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (**ograniczenie celu**),
   4) w sposób przejrzysty dla osoby, której dane dotyczą (**transparentność**),
   5) w konkretnych celach i nie "na zapas" (**minimalizacja**),
   6) w zakresie niezbędnym w stosunku do celów przetwarzania (**adekwatność**),
   7) z dbałością o prawidłowość danych (**prawidłowość**),
   8) przez określony czas, nie dłuższy niż to jest potrzebne (**czasowość – retencja danych**),
   9) zapewniając odpowiednie bezpieczeństwo danych (**bezpieczeństwo**).

6 OBOWIĄZEK INFORMACYJNY:

AnSat w stosunku do osób których dane przetwarza wykonuje tzw. **obowiązek informacyjny** (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody). W tym celu opracowano stosowną procedurę oraz wzory informacji, które udostępnione są pracownikom do stosowania.

7 POWIERZENIE PRZETWARZANIA DANYCH:

W przypadku gdy zajdzie konieczność przekazania danych podmiotowi realizującemu w ramach umowy zadania z AnSat zawierana jest tzw. umowa powierzenia regulująca problematykę określoną w art. 28

RODO. Opracowano stosowną procedurę oraz wzór umowy, które udostępnione są pracownikom do stosowania. Dla potrzeb wewnętrznych AnSat prowadzi wykaz podmiotów z którymi zawarto umowę.

8 REJESTR CZYNNOŚCI PRZETWARZANIA:

Realizując obowiązek wynikający z art. 30 RODO AnSat prowadzi i aktualizuje Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr może zawierać także kolumny nieobowiązkowe, w których rejestruje się informacje dodatkowe ułatwiające zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

9 BEZPIECZEŃSTWO DANYCH

1. AnSat deklaruje, że wdraża i stosuje środki techniczne i organizacyjne adekwatne do zagrożeń naruszenia praw i wolności osób zidentyfikowanych w procesie analizy ryzyka w szczególności: wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. Po przeanalizowaniu komunikatu Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. (Monitor Polski nr 666 z 2019 r.) ustalono, że aktualnie w AnSat nie realizuje się operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony.
3. Dla potrzeb wewnętrznych prowadzony jest wykaz stosowanych zabezpieczeń, a zasady bezpieczeństwa podczas przetwarzania danych określono w procedurach wewnętrznych.
4. Opracowano procedurę pozwalającą na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych.
5. W celu zapewnienia właściwego stosowania środków organizacyjnych i technicznych podczas przetwarzania danych osobowych prowadzone są szkolenia pracowników.
6. Dane osobowe mogą być przetwarzane w AnSat tylko przez osoby mające stosowne upoważnienie wydane przez administratora w trybie określonym procedurą wewnętrzną.
7. W celu oceny, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO w AnSat prowadzone są okresowe audyty.

10 WYZNACZENIE INSPEKTORA OCHRONY DANYCH (IOD)

1. W AnSat wyznaczono Inspektora Ochrony Danych, który w wykonywaniu zadań określonych w art. 39 RODO podlega bezpośrednio właścicielowi PPHU An-Sat – Katarzynie Łakomej.
2. Dane kontaktowe Inspektora Ochrony Danych są publikowane na stronie www oraz dostępne w siedzibie AnSat.
3. IOD odpowiada między innymi za :
    - zapewnienie oraz monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz bezpieczeństwa ich przetwarzania
    - informowanie Administratora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach związanych z RODO
    - nadzór oraz przeprowadzania audytów w AnSat
    - prowadzenie szkoleń pracowników w zakresie ochrony danych osobowych
    - współpraca z organem ochrony danych osobowych we wszystkich sprawach RODO
    - udzielanie zaleceń co do oceny skutków przetwarzania dla ochrony danych zgodnie z art. 35 RODO
    - tworzenie, utrzymywanie oraz aktualizacja rejestrów czynności przetwarzania
    - opracowywanie i aktualizacja dokumentów dotyczących przetwarzania i udostępniania danych, klauzul zgód, poufności oraz informacyjnych
    - rozwiązywanie bieżących problemów oraz rekomendowanie działań związanych z RODO, uzgadnianie poziomu zabezpieczeń i kontrola jakości tych zabezpieczeń.

II. PROCEDURY, WZORY, ZASADY

Niniejszy dział stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu zapewnić wywiązanie się przez Administratora z obowiązków wynikających z RODO w szczególności z art. 32 RODO, czyli zabezpieczeniem przetwarzania danych osobowych przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

1 ZABEZPIECZENIA

1. Wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej.
2. Stosuje się całodobowy monitoring zewnętrzny budynków (tylko klatki wejściowe) należących do Administratora w celu zapewnienia bezpieczeństwa lokatorom.
3. Zainstalowano alarm antywłamaniowy w siedzibie AnSat.
4. Zweryfikowano zakresy danych osobowych przetwarzanych w poszczególnych pomieszczeniach.
5. Rozmieszczenie komputerów, drukarek, ksero ogranicza dostęp osób nieupoważnionych.
6. Dostęp do pomieszczeń (w tym biurowych) zabezpieczono drzwiami zamykanymi na klucz. Dostęp do korytarza łączącej części biurowe zabezpieczono drzwiami zamykanymi na klucz.
7. Dostęp do pomieszczeń biurowych w których przetwarzane są dane osobowe mają tylko upoważnieni pracownicy.
8. W pomieszczeniach zapewniono szafy zamykane. Zapewniono metalową szafę zamykaną na potrzeby przechowywania dokumentacji pracowniczej oraz elektronicznych kopi baz danych. Dostęp do niej ma tylko jedna wyznaczona osoba.
9. Na terenie lokalu zapewniono urządzenia ppoż.
10. W celu ochrony danych przetwarzanych w formie elektronicznej ustalono zasady tworzenia kopii zapasowych.
11. Wdrożono zabezpieczenia systemu informatycznego oraz stacji roboczych według zasad opisanych w Instrukcji Zarządzania RODO.
12. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi ze stacji roboczych są niszczone w sposób fizyczny w tym również komisyjnie, co należy potwierdzić w protokole zniszczenia.
13. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych)
14. Dokumentacja papierowa niszczona jest w niszczarkach paskowych.
15. Informatyk zabezpiecza komputery, systemy informatyczne, poprzez odpowiednią konfigurację, aktualizację aplikacji, ustawienie oprogramowania antywirusowego, firewall, przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.
16. Zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach.
17. Przydzielono indywidualne dostępy do komputerów uprawnionym użytkownikom.
18. Obsługę informatyczną powierzono wykwalifikowanej osobie dającej gwarancję właściwego zabezpieczenia sprzętu informatycznego.

2 UPOWAŻNIENIA

1. Decyzję o upoważnieniu osoby do przetwarzania danych osobowych zgromadzonych w AnSat, zmianie zakresu upoważnienia bądź cofnięciu upoważnienia podejmuje Administrator.

2. Przed udzieleniem upoważnienia należy przeszkolić osobę z zasad ochrony danych osobowych wynikających z przepisów ogólnych oraz regulacji wewnętrznych obowiązujących w AnSat. Potwierdzeniem wykonania obowiązku jest oświadczenie podpisane przez osobę fizyczną.
3. Upoważnienia nadawane są w formie dokumentu wpinanego do akt osobowych pracownika. Upoważnienia osób innych przechowywane są w dokumentacji RODO.
4. Czynności związane z przygotowaniem dokumentu, monitorowanie terminowości jego sporządzenia wykonuje pracownik prowadzący sprawy kadrowe.
5. Upoważnienia mogą być nadawane także w formie poleceń służbowych odnoszących się do jednorazowych czynności wykraczających po za zakres stałego upoważnienia. W celu zapewnienia rozliczalności, polecenie powinno niezwłocznie zostać potwierdzone na piśmie, może to być także wydruk wiadomości elektronicznej.
6. Każda osoba upoważniona musi przetwarzać dane wyłącznie na i w zakresie określonym poleceniem Administratora lub na podstawie przepisu prawa.

Wzór upoważnienia:

U P O W A Ż N I E N I E

Na podstawie Art. 29 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27.04 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. UR L119, S.1), nadaje upoważnienie Panu/i .....

(imię, nazwisko oraz zajmowane stanowisko)

do przetwarzania od dnia ..... danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku.

Jednocześnie zobowiązuję Panią/a do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz przepisami RODO, Ustawy z dnia .10 maja 2018 r. o ochronie danych osobowych, kodeksu pracy a także polityką ochrony danych osobowych pracodawcy.

Jednocześnie upoważniam Panią/a do tworzenia, posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi z zachowaniem pełnej ich ochrony pracy, zastosowania środków technicznych i organizacyjnych Usługi Komunalne Spółka z o.o.

.....

Podpis i pieczęć osoby działającej w imieniu Administratora

Wzór oświadczenia:

…….. ……

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

O Ś W I A D C Z E N I E

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz wdrożonymi wewnętrznymi regulacjami w zakresie ochrony danych– w szczególności Polityką Ochrony Danych Osobowych.

Znany jest mi zakres odpowiedzialności z tytułu nieuprawnionego przetwarzania danych osobowych wynikający z przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

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,
- 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.

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

3 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być przeszkolona / zapoznana z wewnętrznymi zasadami przestrzegania RODO.
2. Szkolenie powinno obejmować część teoretyczną na którą składa się zapoznanie z obowiązującym systemem prawnym oraz wdrożonymi regulacjami wewnętrznymi; a także praktyczną polegającą na wskazaniu stosowanych zabezpieczeń oraz procedur stosowanych w przetwarzaniu udostępnianych pracownikowi danych.
3. Szkolenie przeprowadza Administrator, bądź osoba przez niego wskazana.
4. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą Planu szkolenia RODO, listy uczestników oraz pisemnego potwierdzenia odbycia szkolenia.
5. Po zapoznaniu z zasadami ochrony danych osobowych, uczestnik zobowiązany jest do potwierdzenia znajomości tych zasad i deklaracji ich stosowania. W tym celu stosuje się oświadczenie poufności.

Przykładowy plan szkolenia wewnętrznego:

Zakres szkolenia:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
- Definicje dot. Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.
- Legalność przetwarzania danych osobowych
- Obowiązek informacyjny
- Zasady ujawniania oraz powierzania danych osobowych
- Prowadzenie rejestru czynności przetwarzania
- Przepisy karne
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania
- Przegląd treści Polityki Ochrony Danych Osobowych
- Zabezpieczenia fizyczne obszarów przetwarzania
- Zasady bezpiecznego użytkowania sprzętu IT
- Zasady bezpiecznego korzystania z oprogramowania
- Zasady bezpiecznego korzystania z internetu
- Zasady bezpiecznego korzystania z poczty elektronicznej
- Nadawanie upoważnień do przetwarzania danych osobowych
- instrukcja postępowania w przypadku wystąpienia incydentu
- Postępowanie dyscyplinarne

4 ANALIZA RYZYKA

1. Administrator powołuje zespół do przeprowadzenia analizy ryzyka.
2. Zespół określa listę zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych.
3. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania.
4. Zespół:
   a) określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania (skalę prawdopodobieństwa prezentuje Tabela A),

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

   b) określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne (skalę skutków prezentuje Tabela B),

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

   c) wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S
   d) porównuje wyliczone ryzyka ze skalą i rekomenduje Administratorowi propozycję dalszego postępowania z ryzykiem (skalę Ryzyka prezentuje Tabela C)

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

5. Administrator podejmuje decyzje o zastosowaniu odpowiednich środków adekwatnych do wartości ryzyka
   a) Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
   b) Działania obniżające ryzyko, które może zastosować Administrator:
      - Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie),
      - Unikanie – eliminacja działań powodujących ryzyko,
   c) Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka.

6. Plan postępowania z ryzykiem
   a) Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne sporządzając w tym celu Plan postępowania z ryzykiem.
   b) Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

<u>Wzór planu postępowania z ryzykiem:</u>

PLAN POSTĘPOWANIA Z RYZYKIEM				
Aktywa	**Zagrożenie**	**Proponowane zabezpieczenie**	**Osoba odpowiedzialna**	**Przewidywana data wprowadzenia**

5 UMOWY POWIERZENIA

W celu zapewnienia bezpieczeństwa przetwarzania danych przez podmiot wykonujący usługi na zlecenie i w zakresie określonym przez Administratora konieczne jest uregulowanie w formie pisemnej kwestii prawnych w umowie głównej, bądź umowie dodatkowej. Przykładowy wzór znajduje się poniżej – wymaga on dostosowania do zaistniałej sytuacji.

Treść zawieranej umowy powierzenia należy uzgodnić z Inspektorem Ochrony Danych.

W celu kontroli oraz weryfikacji uprawnień wynikających z powierzenia danych Administrator może prowadzić rejestr zawartych umów powierzenia.

Przykładowy wzór rejestru umów powierzenia:

Lp.	Nazwa Procesora	Kategoria osób których dane dotyczą, kategoria danych osobowych, zakres przetwarzanych danych	Okres na jaki zawarto umowę	Zakres czynności przetwarzania
1				

W przypadku gdy inny podmiot przekaże dane do przetwarzania AnSat w celu realizacji zadań tego podmiotu, to wówczas AnSat wypełni obowiązki wynikające z art. 30 ust. 2 RODO poprzez prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierającego następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie -przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Wzór umowy powierzenia przetwarzania danych osobowych:

Umowa zawarta w ..... w dniu ..... r. pomiędzy:

XXX z siedzibą w ....., zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP ..... oraz numer REGON ....., reprezentowaną/ym przez: ....., zwaną/ym dalej Zleceniodawcą,

a

YYY z siedzibą w ....., zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP ..... oraz numer REGON ....., reprezentowaną/ym przez: ....., zwaną/ym dalej Zleceniobiorcą

§ 1

Definicje

1. Podmiot przetwarzający – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy umowy powierzenia ze Zleceniodawcą, zwany także Zleceniobiorcą

2. Administrator - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych, zwany także Zleceniodawcą

3. Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

4. Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

5. Rozporządzenie- 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 (ogólne rozporządzenie o ochronie danych),

6. Inny podmiot przetwarzający - podmiot, któremu podmiot przetwarzający w imieniu administratora pod-powierzył w całości lub częściowo przetwarzanie danych osobowych

§ 2

Przedmiot Umowy, cel, charakter i zakres

1. Przedmiotem umowy jest powierzenie przez Zleceniodawcę danych osobowych do przetwarzania przez Zleceniobiorcę
2. Celem powierzenia jest:

- świadczenie usług obsługi kadr, płac, księgowości w zakresie danych osobowych pracowników, współpracowników, podwykonawców, kontrahentów
- realizacja usług BHP w zakresie danych osobowych pracowników
- administracja systemami informatycznymi w zakresie danych osobowych przetwarzanych w tych systemach
- hosting poczty, hosting serwerów w zakresie danych osobowych przetwarzanych w tych systemach
- usługa niszczenia dokumentów, archiwizacji w zakresie wszelkich danych osobowych przeznaczonych do niszczenia, przeznaczonych do archiwizacji
- realizacja usług marketingowych w zakresie danych klientów i potencjalnych klientów
- wykonywanie badań laboratoryjnych w zakresie danych wynikowych pacjentów
- obsługa systemu monitoringu wizyjnego

3. Charakter przewarzania danych dotyczy przetwarzania danych osobowych w formie papierowej, przy wykorzystaniu systemów informatycznych.

§ 3

Czas trwania

1. Podmiot przetwarzający uprawniony jest do przetwarzania powierzonych danych do dnia …… /wygaśnięcia lub rozwiązania Umowy głównej.

2. W terminie ….. dni od ustania Umowy, Podmiot przetwarzający zobowiązany jest do usunięcia powierzonych danych, ze wszystkich nośników, programów i aplikacji w tym również kopii, chyba, że obowiązek ich dalszego przetwarzania wynika z odrębnych przepisów prawa.
3. (warunkowo) Podmiot przetwarzający w terminie ….. dni od ustania Umowy zobowiązany jest do zwrotu powierzonych danych na nośnikach papierowych lub elektronicznych

§4

Obowiązki i prawa

1. Zleceniobiorca zobowiązuje się współpracować ze Zleceniodawcą w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą, opisane w rozdziale III Rozporządzenia (w szczególności informowanie i przejrzysta komunikacja, dostęp do danych, obowiązek informacyjny, prawo dostępu, prawo do sprostowania danych, usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, prawo sprzeciwu, zautomatyzowane podejmowanie decyzji).
2. Zleceniobiorca zobowiązuje się do pomocy Zleceniodawcy w wywiązaniu się z obowiązków określonych w art. 32-36 Rozporządzenia (w szczególności dla bezpieczeństwa przetwarzania, zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, przeprowadzania oceny skutków dla ochrony danych osobowych, konsultacji z organem nadzorczym)
3. Zleceniobiorca zobowiązuje się do udostępnienia Zleceniodawcy wszelkich informacji niezbędnych do wykazania spełnienia obowiązków spoczywających na Zleceniobiorcy oraz umożliwi Zleceniodawcy lub audytorowi upoważnionemu przez Zleceniodawcę przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych

§5

Zgłaszanie incydentów

1. Zleceniobiorca zobowiązuje się po stwierdzeniu naruszenia ochrony danych osobowych do zgłoszenia tego Zleceniodawcy bez zbędnej zwłoki
2. Informacja przekazana Zleceniodawcy powinna zawierać co najmniej:

a. opis charakteru naruszenia oraz - o ile to możliwe - wskazanie kategorii i przybliżonej liczby osób, których dane zostały naruszone i ilości/rodzaju danych, których naruszenie dotyczy

b. opis możliwych konsekwencji naruszenia,

c. opis zastosowanych lub proponowanych do zastosowania przez Zleceniobiorcę środków w celu zaradzenia naruszeniu, w tym minimalizacji jego negatywnych skutków.

§ 6

(paragraf warunkowy – pozostaje, gdy występuje podopowierzenie)

Korzystanie przez Zleceniobiorcę z usług innego podmiotu przetwarzającego

1. Zleceniobiorca w ramach realizacji Umowy korzysta z usług innego podmiotu przetwarzającego a Zleceniodawca przyjmuje to do wiadomości i wyraża na to zgodę
2. W przypadku zmian dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, Zleceniodawca jest zobowiązany do poinformowania o tym Zleceniodawcę
3. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Zleceniodawcy za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Zleceniobiorcy

§7

Deklarowane środki techniczne i organizacyjne

(sugerowane poniższe zapisy powinny znaleźć się w tejże umowie powierzenia)

1. Zleceniobiorca gwarantuje, że każda osoba realizująca Umowę zobowiązana jest do bezterminowego zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy, a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym. Jednocześnie każda osoba realizująca Umowę zobowiązana jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
2. Zleceniobiorca deklaruje stosowanie środków technicznych i organizacyjnych określonych w art. 32 Rozporządzenia, jako adekwatnych do zidentyfikowanego ryzyka naruszenia praw lub wolności powierzonych danych osobowych a w szczególności:

a. pseudonimizację i szyfrowanie danych osobowych;

b. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

3. Zleceniobiorca zobowiązuje się stosować ochronę powierzonych danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

§7a

Szczegółowe deklarowane środki techniczne i organizacyjne

(przykład szczegółowej listy wymagań dla usługi administracji - serwisu IT – „jeśli istnieje potrzeba uszczegółowienia innych zakresów umów – poniżej należy stworzyć dedykowaną listę zabezpieczeń, którą Administrator oczekuje od Podmiotu przetwarzającego")

1. Zleceniobiorca zobowiązuje się dopuszczać do przetwarzania danych osobowych osoby realizujące Umowę (podać ewentualnie funkcje osób, serwisanci, konsultanci, …..) poinformowane i przeszkolone z zasad bezpieczeństwa pracy z danych osobowymi
2. Każda osoba realizująca Umowę zobowiązana jest do przetwarzania danych osobowych do których uzyskała dostęp wyłącznie w zakresie i celu przewidzianym w Umowie.
3. Każda osoba realizująca Umowę zobowiązana jest do zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym.
4. Każda osoba realizująca Umowę zobowiązuje się do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
5. Każda osoba realizująca Umowę zobowiązana jest do nie powodowania niezgodnych z Umową zmian danych lub utraty, uszkodzenia lub zniszczenia tych danych.
6. Każda osoba realizująca Umowę zobowiązuje się do niedokonywania jakiegokolwiek kopiowania i utrwalania danych osobowych poza systemami informatycznymi Zleceniodawcy
7. W przypadku wykorzystania sieci publicznej, każda osoba realizująca Umowę zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego (VPN, SSL, podać inne).
8. Każda osoba realizująca Umowę zobowiązuje się do pracy w systemach Zleceniodawcy z użyciem uwierzytelnienia

§8

Postanowienia końcowe

1. Umowa zastępuje wszelkie inne ustalenia dokonane pomiędzy Zleceniobiorcą a Zleceniodawcą dotyczące przetwarzania danych osobowych bez względu na to, czy zostały uregulowane umową czy innym instrumentem prawnym.
2. W zakresie nieuregulowanym Umową mają zastosowanie przepisy prawa obowiązującego na terenie Rzeczypospolitej Polskiej, w tym Rozporządzenia.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

....

6 INFORMOWANIE O PRZETWARZANIU DANYCH

Administrator realizuje obowiązek informacyjny względem osób fizycznych poprzez udzielanie im informacji o zasadach przetwarzania danych osobowych w trybie art. 13 bądź 14 RODO na zasadach określonych w art. 12 RODO.

Każdy z pracowników wykonujący czynności prowadzące do pozyskania danych osobowych zobowiązany jest do opracowania informacji w oparciu o poniższy wzór.

Zmiana treści informacji w szczególności: celu przetwarzania, podstawy przetwarzania, praw osoby wymaga poinformowania osoby fizycznej o treści objętej zmianą.

Czuwanie nad prawidłowością sporządzenia informacji oraz wywiązanie się z obowiązku jej udzielenia należy do każdego pracownika w zakresie wynikającym z realizowanych przez niego czynności przetwarzania danych. Treść i poprawność informacji należy uzgodnić z IOD.

Administrator zatwierdza do stosowania opracowane informacje o przetwarzaniu danych osobowych oraz aprobuje sposób jej udostępnienia osobie której dane są przetwarzane

Informacje dla osób niebędących pracownikami AnSat udostępnia się na stronie www Administratora.

Administrator zapewnia, że informacja o zasadach przetwarzania danych w celu realizacji przez Administratora jego zadań zamieszczana jest na stronie www, tablicy ogłoszeń w siedzibie AnSat oraz w miejscach pozyskiwania danych.

Wzory informacji:

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Miejska Spółdzielnia Mieszkaniowa we Wrocławiu z siedzibą we Wrocławiu przy ul. Prądzyńskiego 14-16
2) kontakt z Inspektorem Ochrony Danych możliwy jest elektronicznie pisząc adres email kancelaria@dcw.wroclaw.pl bądź na podany wyżej adres Spółdzielni
3) Pani/Pana dane osobowe przetwarzane będą w celu……
4) Podstawą przetwarzania danych jest …….. (określić z uwzględnieniem Art. 6 ust. 1 lit. a, b, c, d, e, f lub Art.9 ust.1 lit. a, b, c, d, h, i, j - ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.) jeżeli podstawą legalności jest art. 6 ust. 1 lit. f) (czyli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią) – to należy wskazać ten uzasadniony interes
5) odbiorcami Pana/Pani danych osobowych będą (podać informacje o odbiorcach lub kategoriach odbiorców jeżeli istnieją) *
6) Pana/Pani dane osobowe przechowywane będą przez okres …..dni/lat (lub kryteria ustalania okresu)
7) posiada Pani/Pan prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie*
8) ma Pan/Pani prawo wniesienia skargi do organu nadzorczego
9) podanie danych osobowych jest wymogiem ustawowym/umownym/warunkiem zawarcia umowy/ dobrowolne/ *, jednakże niepodanie danych w zakresie wymaganym przez administratora może skutkować……

10) Pana/Pani dane będą/nie będą poddane zautomatyzowanym podejmowaniu decyzji (profilowaniu) w celu ……, (podać przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą)

Zgodnie z art. 14 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Miejska Spółdzielnia Mieszkaniowa we Wrocławiu z siedzibą we Wrocławiu przy ul. Prądzyńskiego 14-16
2) kontakt z Inspektorem Ochrony Danych możliwy jest elektronicznie pisząc adres email kancelaria@dcw.wroclaw.pl bądź na podany wyżej adres Spółdzielni
3) Pani/Pana dane osobowe przetwarzane będą w celu……
4) Podstawą przetwarzania danych jest …….. (określić z uwzględnieniem Art. 6 ust. 1 lit. a, b, c, d, e, f lub Art.9 ust.1 lit. a, b, c, d, h, i, j - ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.) jeżeli podstawą legalności jest art. 6 ust. 1 lit. f) (czyli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią) – to należy wskazać ten uzasadniony interes
5) kategoria danych osobowych: dane wrażliwe/niewrażliwe *
6) Pana/Pani dane osobowe pozyskano z…… (podać źródło [w tym źródło publiczne])
7) odbiorcami Pana/Pani danych osobowych będą…… (podać nazwę odbiorców lub kategorię odbiorców jeżeli istnieją) *
8) Pana/Pani dane osobowe przechowywane będą przez okres …..dni/lat (lub kryteria ustalania okresu)
9) posiada Pani/Pan prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawie do cofnięcia zgody w dowolnym momencie*
10) ma Pan/Pani prawo wniesienia skargi do organu nadzorczego
11) Pana/Pani dane będą poddane zautomatyzowanym podejmowaniu decyzji (profilowaniu) w celu ……, (podać przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą)
12) Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane: Pana/Pani dane będą przetwarzane w celu ……..
13) Pani/Pana dane będą przekazane odbiorcy w państwie trzecim lub organizacji międzynarodowej

Przykłady informacji – do uzupełnienia:

Dla umów-zleceń, umów o dzieło oraz z kontrahentami (CEIDG)

Zgodnie z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) zwanym dalej RODO informuję, iż:

1) administratorem Pani/Pana danych osobowych jest Miejska Spółdzielnia Mieszkaniowa we Wrocławiu z siedzibą we Wrocławiu przy ul. Prądzyńskiego 14-16
2) kontakt z Inspektorem Ochrony Danych możliwy jest elektronicznie pisząc adres email kancelaria@dcw.wroclaw.pl bądź na podany wyżej adres Spółki
3) Pani/Pana dane osobowe przetwarzane będą w celu niezbędnym do doprowadzenia do zawarcia umowy, bądź jej realizacji. Administrator może wykorzystać także dane w zakresie koniecznym do wypełnienia obowiązków prawnych jakie wiążą się z zawarciem umowy.
4) Podstawą przetwarzania danych jest czynność prowadząca do zawarcia umowy bądź zawarta umowa (zgodnie z art. 6 ust. 1 lit. b RODO).
5) odbiorcami Pani/Pana danych osobowych będą podmioty uprawnione do uzyskania danych osobowych lub Podmioty uczestniczące w realizacji zlecenia
6) Pani/Pana dane osobowe przechowywane będą przez okres realizacji umowy i 5 lat od jej zakończenia.
7) posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.
8) ma Pani/Pan prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych
9) podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych może skutkować odmową zawarcia umowy

* niepotrzebne skreślić

Sposób wprowadzenia/umieszczenia pełnej klauzuli informacyjnej

- w zamówieniu do dostawcy lub do klienta
- w umowie w postaci stopki
- w postaci stopki na fakturze
- w stopce maila do tej osoby
- na stronie www

7 ZGODY

W przypadkach wymagających pozyskania zgody od osoby fizycznej na przetwarzanie jej danych osobowych należy postępować zgodnie z niniejszymi zasadami.

Definicja zgody wg RODO: zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Wymogi zgody (zgodnie z definicją):

- **dobrowolność**: należy rozumieć jako brak przymusu i **możliwość odmowy wyrażenia zgody**; zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą. Zgodnie z motywem 43 RODO - zgody nie uważa się za dobrowolną, jeżeli nie **można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych**, mimo że w danym przypadku byłoby to stosowne. Zgoda nie będzie dobrowolna także w sytuacji, w której stanowi uzależnienie świadczenia drugiej strony.
- **konkretność**: wymóg powiązany z treścią zgody i celem przetwarzania; zgodnie z motywem 32 RODO zgoda **powinna dotyczyć wszystkich czynności przetwarzania** dokonywanych w tym samym celu lub w tych samych celach, natomiast jeżeli przetwarzanie służy **różnym celom, potrzebna jest osobna zgoda na wszystkie te cele;**
- **świadomość**: zakłada, że osoba jest poinformowana i powinna zdawać sobie sprawę z konsekwencji swojego działania- motyw 42 RODO „aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych"
- **jednoznaczność**: przyzwolenie na przetwarzanie danych nie może budzić wątpliwości co do zamiaru osoby, która takie działanie podejmuje.

Warunki wyrażenia zgody według art. 7 RODO:

- Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę (przyp. aut. przy spełnieniu ww. zasad i warunków wynikających z definicji i motywów RODO odnoszących się do zgody) - na przetwarzanie swoich danych osobowych (przyp. aut. zasada rozliczalności).
- jeżeli zgoda jest częścią pisemnego oświadczenia, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.
- osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę – co więcej należy o tym poinformować zanim osoba wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
- zgodę wyrażona jest dobrowolnie – m.in. od zgody na przetwarzanie danych nie może być uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

W związku z zasadą przejrzystości, zastosowanie będą mieć także takie wymogi jak zwięzłe, łatwo dostępne i zrozumiałe, a w stosownych przypadkach, dodatkowo wizualizowane komunikaty.

UWAGA: dla usprawnienia pracy należy zadbać o to żeby uregulować kwestie zgody oraz informacyjne już w dokumentach aplikacyjnych, wzorach wniosków składanych do AnSat.

UWAGA: przetwarzając dane na podstawie zgody należy wprowadzić zmiany do klauzuli informacyjnej.

Przykładowy wzór zgody:

Zgodnie z art.6 ust.1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. wyrażam zgodę na przetwarzanie moich danych osobowych …….. w celu ……

Zostałem/am poinformowany/a o przysługującym mi prawie do cofnięcia zgody w dowolnym momencie – wiem, że cofnięcie zgody nie wpływa na zgodność z prawem czynności dokonanych przed jej cofnięciem.

Data i podpis .....

8 REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. W celu zapewnienia możliwości skorzystania przez osoby fizyczne z uprawnień przewidzianych w art. 15 – 22 RODO, Administrator określa zasady postępowania w celu zapewnienia sprawnego ustosunkowania się do zgłoszonego żądania.
2. Osoba fizyczna zamierzając skorzystać z przysługującego mu uprawnienia powinna złożyć wniosek w tej sprawie na piśmie w sekretariacie AnSat, przesłać go do siedziby w formie papierowej bądź elektronicznie na adres biuro@an-sat.pl.
3. W przypadku złożenia żądania słownie osoba proszona jest o potwierdzenie żądania na piśmie, w celu jego udokumentowania.
4. Każde zgłoszenie należy przekazać do Administratora, który podejmuje decyzję o sposobie jego realizacji.
5. W przypadkach tzw. nagłych Administrator zapewnia ograniczenie przetwarzania danych do czasu sprawdzenia okoliczności i podstaw żądania.
6. Administrator informuje osobę o podjętych działaniach w terminie miesiąca od otrzymania żądania. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

9 POZYSKIWANIE DANYCH Z SIECI

W celu realizacji obowiązków ustawowych Administrator może pozyskiwać dane z punktów końcowych swojej sieci multimedialnej w celu przekazywania ich do UKE poprzez systemy informatyczne i diagnostykę sieci; pozyskane dane podlegają częściowej pseudoanonimizacji.

AnSat deklaruje, że zbiera tylko dane niezbędne do prawidłowego sporządzania sprawozdań do UKE.

Administrator zobowiązuje pracowników AnSat do właściwego zabezpieczenia zgromadzonych danych, oraz informatyka do nadzoru nad zabezpieczeniem urządzeń informatycznych w sposób gwarantujący bezpieczeństwo przetwarzanych danych.

10 AUDYTY

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

1. O przeprowadzeniu audytu z roczną częstotliwością lub częściej decyduje Administrator określając rodzaj audytu (wewnętrzny/zewnętrzny).
2. Administrator określa zakres audytu biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
3. Administrator wyznacza audytora do przeprowadzenia audytu.
4. Audytor jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów.

5. Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.
6. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia oraz rekomenduje podjęcie odpowiednich działań.
7. Wynik audytu zostaje udokumentowany przez audytora i przekazany Administratorowi.
8. Administrator wraz z IOD dokonuje przeglądu i analizy wyniku audytu oraz decyduje o uruchomieniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

11 INCYDENTY

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

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania Administratora bądź Inspektora Ochrony Danych o stwierdzeniu podatności lub wystąpieniu incydentu.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu IOD prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   2) inicjuje ewentualne działania dyscyplinarne,
   3) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
   4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia,
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, skutki oraz podjęte działania zaradcze.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku ustalenia, iż naruszenie ochrony danych osobowych prawdopodobnie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.
8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Wzór Rejestru incydentów / naruszeń:

Lp.	Opis / okoliczności naruszenia/incydentu	Ilość osób dotknięta naruszeniem / incydentem	Skutki naruszenia /incydentu	Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Osoba odpowiedzialna za wdrożenie działań

Lp.	Opis / okoliczności naruszenia/incydentu	Ilość osób dotknięta naruszeniem / incydentem	Skutki naruszenia /incydentu	Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Osoba odpowiedzialna za wdrożenie działań
1							
2							

W celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych Administrator wprowadza poniższe zasady obowiązujące:

- Pracowników.
- Współpracowników (osoby wykonujące w AnSat pracę na innej podstawie niż umowa o pracę).
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora.
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora.

12 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, PROGRAMÓW

Administrator wdrożył zabezpieczenia organizacyjne i techniczne odpowiadające zagrożeniu dla bezpieczeństwa danych przetwarzanych w systemie informatycznym. W tym celu opracował Instrukcję Zarzadzania Systemem Informatycznym, której realizacja powierzona została Informatykowi.

Użytkownicy SZSI zobowiązani są do przestrzegania określonych zasad oraz wdrożonych rozwiązań w szczególności:

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT
3. Samowolne instalowanie, otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
5. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce). Skuteczny sposób zniszczenia twardego dysku, pendrive Użytkownik jest zobowiązany uzgodnić z informatykiem.
6. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych.
7. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.

8. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie Administratora wykonywane przez informatyka.
9. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
10. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
11. Zabrania się pracy wielu użytkowników na wspólnym koncie.
12. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
13. Użytkownik jest zobowiązany do powiadomienia Administratora i informatyka o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje
14. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym informatyka.
15. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu
16. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
17. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako informatyk. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
18. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy.

13 ZASADY POSŁUGIWANIA SIĘ HASŁAMI

1. Hasła powinny składać się z co najmniej 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Hasła muszą być zmieniane co 30 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym AnSat.
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

14 ZASADY ZABEZPIECZANIA DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Pracownicy upoważnieni do przetwarzania danych są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w

szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach socjalnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

15 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA AN-SAT

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora. Do takich nośników zalicza się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zabezpieczone hasłem pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w torbach, teczkach.
4. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą
5. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą,
    c. stosować bezpieczne koperty depozytowe,
    d. przesyłkę należy przesyłać przez kuriera.
6. W przypadku korzystania z usług firm kurierskich, należy wybierać te które dają gwarancję bezpieczeństwa oraz działają w oparciu o przepisy regulujące dostarczanie przesyłek.
7. Bez zgody Administratora nie wolno umieszczać plików z danymi w usługach chmury obliczeniowej. W przypadku wyrażenia takiej zgody plik należy zabezpieczyć hasłem.

16 ZASADY KOPIOWANIA DANYCH

1. Użytkownicy nie mogą bez zgody Administratora kopiować danych w celu innym niż służbowy.
2. Kopiowanie dokumentów z danymi należy ograniczyć do ilości koniecznej wynikającej z zasad prowadzenia korespondencji bądź wymogów prawnych.
3. Niedopuszczalne jest kopiowanie dokumentów z danymi w nadmiarze i pozostawianie ich w miejscach niezabezpieczonych.
4. Kopiowanie, rozpowszechnianie danych w całości lub w części bez zgody Administratora w celu wyniesienia, wysłania ich po za obszar przetwarzania tj. siedziba AnSat traktowane będzie jako kradzież i podlega zgłoszeniu do organów ścigania.

17 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora bądź informatyka i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron

tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

18 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza AnSat może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza AnSat należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zabezpieczone hasłem, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 10 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. WAŻNE: Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.
7. WAŻNE: Nie wolno „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hiperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.
8. Należy zgłaszać informatykowi przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych” emaili w formie „łańcuszków szczęścia".
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”
11. Użytkownicy powinni okresowo kasować niepotrzebne maile.
12. Konta pocztowe służbowe nie mogą być połączone z pocztą prywatną.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
17. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

18. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
20. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące AnSat, jej pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

19 OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

III. OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY 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 Administratora zadaniach.
    b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Administratora.
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora.
    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. Osoby zapoznane z treścią niniejszej Polityki lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
3. 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.
4. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
5. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta organizacja, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

IV. POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

V. POSTANOWIENIA KOŃCOWE

Pracownicy oraz współpracownicy, którzy zapoznali się z treścią Polityki Ochrony Danych Osobowych w PPHU An-Sat Katarzyna Łakoma potwierdzają ten fakt swoim podpisem na „Karcie zapoznania z dokumentem", która stanowi załącznik nr 1 do niniejszej Polityki.