Kyrylo Radionov

ul. Gagarina 19/332

87-100 Toruń

POLITYKA OCHRONY DANYCH OSOBOWYCH

Niniejsza polityka obowiązuje od dnia 25/05/2018r w firmie Kyrylo Radionov

Podstawą wprowadzenia niniejszego dokumentu jest 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) (Dz.U.UE.L.2016.119.1).

SPIS TREŚCI

I. WSTĘP

§ 1.

1. Działając na podstawie Rozporządzenie Parlamentu Europejskiego i Rady Europy UE 2016/679 z dnia 27-04-2016 r. zwanego dalej RODO Administrator, postanowił wdrożyć politykę ochrony danych osobowych w swojej firmie Kyrylo Radionov , aby zminimalizować mogące wystąpić zagrożenia w tym:
   a. naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie, ataki z Internetu, przypadkowe lub celowe rozproszenie, scalenie, przetwarzanie danych w Internecie z ominięciem zabezpieczeń Systemu informatycznego lub wykorzystaniem luk i błędów systemów informatycznych Administratora;
   b. sytuacje spowodowane z zamiarem umyślnym lub losowe oraz nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu informatycznego, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie;
   c. czynniki zakłócające (parametry otoczenia) pracę urządzeń komputerowych (nadmierna wilgotność, niska lub bardzo wysoka temperatura, oddziaływanie pola elektrycznego i elektromagnetycznego itp.)
   d. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie procedur serwisowych w tym przyzwolenie na naprawę sprzętu zawierającego Dane osobowe poza siedzibą Administratora;
   e. udostępnienie osobom nieupoważnionym zasad ochrony danych stosownych przez Administratora,
   f. naruszenia zasad określonych w polityce z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem zasad ochrony danych, w tym zwłaszcza:
      - nie wykonywanie zapasowych kopi zgodnie z przyjętymi u Administratora procedurami:
      - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy;
      - naruszenie bezpieczeństwa danych przez nieautoryzowane ich Przetwarzanie;
      - ujawnienie osobom nieupoważnionym zasad ochrony danych stosowanych u Administratora;
      - ujawnienie osobom nieupoważnionym danych przetwarzanych przez Administratora, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru w niedostatecznie nadzorowanych pomieszczeniach Administratora:
      - Przetwarzanie danych osobowych niezgodnie z celem określonym przez Administratora, w szczególność w celach marketingowych handlowych i celów prywatnych;
      - wprowadzanie zmian do Systemu informatycznego Administratora i instalowanie jakiegokolwiek oprogramowania bez zgody ASI.

§ 2.

Słownik (objaśnienie skrótów)

1) Administrator– rozumie się przez to osobę odpowiedzialną za bezpieczeństwo informacji chronionych, ustalającą/ustalającego cele i sposoby przetwarzania danych osobowych .

2) Inspektor Ochrony Danych (IOD) - oznacza osobę, której administrator danych powierzył realizację zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, osoba ta pełni także funkcje doradczą w zakresie polityki bezpieczeństwa danych osobowych.

3) Administrator Systemu Informatycznego (ASI) – oznacza wyznaczoną przez Administratora osobę nadzorującą pracę Systemu informatycznego posiadającą odpowiednie kwalifikacje .

4) Anonimizacja – oznacza takie przekształcenie danych osobowych, po którym niemożliwe jest przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej, przy czym proces ten jest nieodwracalny;

5) Pseudonimizacja - przetwarzanie danych osobowych w taki sposób by nie było można przypisać je danej osobie, której dane dotyczą, bez użycia dodatkowych informacji pod warunkiem, że takie dodatkowe informacje przechowywane są osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie konkretnej osobie;

6) Członek personelu – oznacza osobę zatrudnioną u Administratora na podstawie stosunku pracy, umów cywilnoprawnych (np. umowy o dzieło lub umowy zlecenia), przedsiębiorcę wykonującego działalność osobiście i jednoosobowo (w tym w ramach umów o współpracy), osobę odbywającą praktyki, stażystę, osobę skierowaną do pracy w ramach umów z agencjami pracy tymczasowej wykonującą pracę związaną z Przetwarzaniem danych osobowych u Administratora;

7) Dane osobowe – oznacza informacje o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (**„osoba, której Dane dotyczą”**). Osobą możliwą do zidentyfikowania jest 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 (art. 4 RODO)

8) Szczególne kategorie Danych osobowych (sensytywne – wrażliwe)– oznacza dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby,

9) Dane dotyczące wyroków i naruszeń prawa - dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;

10) Dane osobowe zwykłe –oznacza dane nie wymienione w punkcie 8 i 9

11) Hasło – oznacza to ciąg znaków cyfrowych ,literowych, lub innych, znany jedynie Użytkownikowi;

12) Identyfikator – oznacza to ciąg znaków cyfrowych literowych, cyfr lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w Systemie informatycznym;

13) Integralność i poufność danych – oznacza to właściwość zapewniającą odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem Przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

14) Komisja – rozumie się przez to Komisję Europejską

15) Odbiorca danych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się Dane osobowe, w tym procesora, z wyjątkiem

organów publicznych, które mogą otrzymywać Dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem polskim

16) Ograniczenie przetwarzania– rozumie się przez to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

17) Organ nadzorczy PUODO – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych

18) Organizacja międzynarodowa – rozumie się przez to organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy,

19) Osoba upoważniona do przetwarzania danych osobowych – rozumie się przez to pracownika , który został upoważniony przez Administratora do przetwarzania danych osobowych u Administratora;

20) Powierzenie przetwarzania danych osobowych – oznacza to zlecenie wykonania czynności przetwarzania danych osobowych przez procesora na rzecz Administratora na podstawie stosownego postanowienia w umowie, zapewniającego warunki bezpieczeństwa danych osobowych zgodnie z przepisami RODO lub na podstawie odrębnej pisemnej umowy powierzenia przetwarzania danych osobowych zawartej zgodnie z art. 28 ust. 3 Rozporządzenia;

21) Procesor – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza Dane osobowe w imieniu Administratora,

22) Przetwarzanie danych – rozumie się przez to 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;

23) Rozliczność – rozumie się przez to właściwość zapewniającą możliwość wykazania przestrzegania przepisów Rozporządzenia;

24) Rozporządzenie – rozumie się przez to 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) (Dz. Urz. UE L 119, s. 1)**(w skrócie** RODO**)**

25) System informatyczny Administratora– rozumie się przez to serwer oraz sprzęt komputerowy, oprogramowanie, Dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, zasad przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych w firmie administratora .

26) Ujawnianie danych osobowych – rozumie się przez to przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie danych osobowych;

27) Usuwanie danych – rozumie się przez to zniszczenie, zamazywanie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której Dane dotyczą;

28) Uwierzytelnianie– rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby fizycznej lub podmiotu;

29) Użytkownik – rozumie się przez to członka personelu upoważnionego na piśmie do przetwarzania danych osobowych, któremu ASI nadał Identyfikator i przyznał Hasło;

30) Zabezpieczenie Systemu informatycznego – rozumie się przez to wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych i informatycznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;

31) Zbieranie danych osobowych – rozumie się przez to pozyskiwanie danych od osoby, której one dotyczą lub z innych źródeł;

32) Zgoda osoby, której Dane dotyczą – rozumie się przez to 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;

33) Firma – rozumie się przez to: Kyrylo Radionov

§ 3.

1. Administrator jest osobą prawną : Kyrylo Radionov
2. Administrator wyznaczył ASI w osobie: …….
3. Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:
   a. Inspektor Ochrony Danych wyznaczony przez Administratora w osobie: ……
   b. komórka audytu wewnętrznego/ komórka odpowiedzialna za obszar bezpieczeństwa informacji;
4. Administrator przetwarza Dane osobowe w sposób tradycyjny (papierowy) oraz w sposób częściowo zautomatyzowany tj. przy użyciu Systemów informatycznych, w tym z wykorzystaniem usług chmurowych, zarówno w Systemach zintegrowanych, jak i w rozproszonych zestawieniach.

II. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

§ 4.

1. Przestrzegając zasad dotyczących przetwarzania Danych osobowych, Administrator zapewnia, by Dane były:
   a. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której Dane dotyczą ("**zgodność z prawem, rzetelność i przejrzystość**"),
   b. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ("**ograniczenie celu**");
   c. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("**minimalizacja danych**");
   d. prawidłowe i w razie potrzeby uaktualniane; Administrator podejmuje wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("**prawidłowość**");
   e. przechowywane w formie umożliwiającej identyfikację osoby, której Dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których Dane te są przetwarzane; ("**ograniczenie przechowywania**");

f. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem Przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("**integralność i poufność**").

2. Przetwarzanie Danych osobowych możliwe jest w przypadku spełnienia jednej z przesłanek określonych w art. 6 ust. 1 lit. a-f Rozporządzenia, tj. w przypadku, gdy:
   a. osoba, której Dane dotyczą wyraziła zgodę na Przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b. 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;
   c. Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   d. Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innej osoby fizycznej;
   e. Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   f. 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, w szczególności gdy osoba, której Dane dotyczą, jest dzieckiem.
3. Przetwarzanie Szczególnych kategorii Danych osobowych jest zabronione, chyba że spełniony jest jeden z warunków określonych w art. 9 ust. 1 lit. a-j Rozporządzenia, tj. w przypadku, gdy:
   a. osoba, której Dane dotyczą, wyraziła wyraźną zgodę na Przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której Dane dotyczą, nie może uchylić zakazu, o którym mowa powyżej;
   b. Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której Dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której Dane dotyczą;
   c. Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której Dane dotyczą, lub innej osoby fizycznej, a osoba, której Dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
   d. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że Przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że Dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których Dane dotyczą;

e. Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której Dane dotyczą;
f. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
g. Przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której Dane dotyczą;
h. Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania Systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem odpowiednich warunków i zabezpieczeń;
i. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
j. Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1Rozporządzenia, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której Dane dotyczą;

§ 5.

1. Administrator na żądanie współpracuje z PUODO w ramach wykonywania przez niego swoich zadań, w szczególności na jego żądanie udostępnia mu rejestr czynności przetwarzania w celu monitorowania operacji przetwarzania.
2. Za współpracę z PUODO odpowiedzialny/a jest Inspektor Ochrony Danych/ wyznaczona przez Administratora do zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa.

§ 6.

1. Administrator śledzi wytyczne, zalecenia oraz najlepsze praktyki określone przez Europejską Radę Ochrony Danych na podstawie art. 70 ust. 1 lit. d-j i m Rozporządzenia i uwzględnia je w swoich działaniach związanych z Przetwarzaniem danych.

III. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

§ 7.

1. Zgodnie z art. 35 RODO Administrator wykonuje swoje obowiązki przestrzegając zasady podejścia opartego na ryzyku. W szczególności jest zobowiązany do przeprowadzenia analizy procesów przetwarzania i dokonania ogólnej oceny ryzyka, jakie wiąże się z Przetwarzaniem Danych w konkretnym przypadku, ze szczególnym uwzględnieniem ryzyka dla praw lub wolności osób, których Dane dotyczą. Po dokonaniu analizy charakteru i kontekstu przetwarzania danych osobowych u Administratora nie zachodzi podstawa zastosowania do dokonania oceny skutków do ochrony danych. Firma zatrudniająca mniej niż 250 osób – nie mniej jednak dokonano analizy ryzyka.
2. Po weryfikacji kontekstu przetwarzania Danych osobowych, w szczególności określeniu procesów, w ramach których Dane są przetwarzane, celów przetwarzania, zaangażowanych podmiotów wewnętrznych i zewnętrznych, zakresu i podstawy przetwarzania, a także używanych narzędzi i stosowanych zabezpieczeń, Administrator określa zakres oceny ryzyka, a także dobiera aspekty kluczowe i metodykę ocenną (Jako podstawa dla przyjętej w RODO konstrukcji obowiązków, omawiany mechanizm realizowany jest poprzez ilościową metodę analizy ryzyka: *prawdopodobieństwo-skutek*)

§ 8.

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania Danych osobowych w strukturach Administratora oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby Przetwarzanie odbywało się zgodnie z Rozporządzeniem, i aby móc to wykazać środki te są w miarę potrzeby poddawane przeglądom i uaktualniane.
2. Realizując swoje obowiązki Administrator współpracuje z Inspektorem Ochrony Danych, Procesorami i osobami, których Dane dotyczą, a także organem nadzorczym.
3. Administrator realizuje zadania w zakresie ochrony Danych osobowych, zmierzające do zapewnienia przestrzegania przepisów Rozporządzenia, w tym w szczególności:
   a. nadzoruje opracowanie i aktualizację dokumentacji ochrony Danych osobowych;
   b. nadzoruje przestrzeganie zasad określonych w dokumentacji ochrony Danych osobowych;
   c. zapewnia adekwatne do zagrożeń i kategorii przetwarzanych Danych osobowych środki techniczne i organizacyjne zapewniające ochronę danych osobowych,
   d. zabezpiecza Dane osobowe przed:
      - ujawnieniem osobom nieupoważnionym;
      - zabraniem przez osobę nieuprawnioną;
      - zmianą, utratą, uszkodzeniem lub zniszczeniem;
   e. zapewnia legalność przetwarzania Danych osobowych, a w szczególności dba, by:
      - Dane osobowe przetwarzane były na podstawie jednej z przesłanek legalizujących Przetwarzanie, które to przesłanki wymienione są w art. 6 ust. 1 lit. a-f albo w art. 9 ust. 2 lit. a-j Rozporządzenia;

- został spełniony wobec osoby, której Dane dotyczą obowiązek informacyjny, o którym mowa w art. 13 i 14 Rozporządzenia;
- Dane osobowe były przetwarzane zgodnie z obowiązującymi przepisami prawa, dobrymi praktykami i zwyczajami oraz normami i zasadami współżycia społecznego;
- Dane osobowe przetwarzane były zgodnie z zasadami określonymi w § 4 ust. 1 Polityki;

f. jeżeli zachodzą przesłanki określone w § 42 powołuje, a w pozostałych przypadkach może powołać w swojej strukturze Inspektora Ochrony Danych, odpowiedzialnego za nadzór nad Przetwarzaniem Danych osobowych zgodnie z przepisami o ochronie danych osobowych;
g. powołuje ASI jako osobę odpowiedzialną za bezpieczeństwo Systemów informatycznych służących do przetwarzania Danych osobowych oraz określa zakres jego zadań;
h. zapewnia zapoznanie osób, którym mają być nadane upoważnienia do przetwarzania Danych osobowych, z przepisami o ochronie danych osobowych oraz zasadami ochrony danych osobowych poprzez zorganizowanie dla nich szkolenia, prowadzonego przez osobę posiadającą odpowiednią wiedzę i kompetencje z zakresu ochrony danych osobowych;
i. upoważnia Członków personelu do przetwarzania Danych osobowych w określonym indywidualnie zakresie;
j. nadzoruje i dba o zgodne z prawem przekazywanie Danych osobowych (Udostępnianie i Powierzanie);
k. zapewnia Użytkownikom odpowiednie stanowiska pracy, w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z prawem Przetwarzanie Danych osobowych;
l. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zasad bezpiecznego przetwarzania Danych osobowych;

4. Administrator gwarantuje poszanowanie praw osób, których Dane dotyczą, a w szczególności prawa do uzyskania informacji o:
   - Administratorze;
   - celu, zakresie i sposobie przetwarzania danych osobowych;
   - terminie od kiedy i jakie Dane osobowe są przetwarzane;
   - źródle, z którego Dane osobowe pochodzą;
   - sposobie ujawniania danych osobowych oraz ich Odbiorcach.
5. Administrator gwarantuje respektowanie praw osób, których Dane dotyczą, w zakresie:
   - żądania sprostowania lub uaktualnienia Danych osobowych;
   - żądania ograniczenia przetwarzania Danych osobowych;
   - wniesienia sprzeciwu wobec przetwarzania Danych osobowych;
   - żądania usunięcia Danych osobowych;
   - żądania potwierdzenia przetwarzania, dostępu do Danych osobowych i uzyskania ich kopii;
   - żądania przeniesienia Danych osobowych;
   - odwołania zgody na Przetwarzanie Danych osobowych;
   - zaniechania zautomatyzowanego podejmowania decyzji.

§ 9.

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym

prawdopodobieństwie wystąpienia i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym 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.

2. Stosowane przez Administratora zabezpieczenia ochrony fizycznej Danych osobowych opisane są w załączniku do Polityki.
3. Stosowane przez Administratora zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej dla fizycznych elementów Systemu, ich połączeń oraz Systemów operacyjnych opisane są w załączniku do Polityki.
4. Stosowane przez Administratora zabezpieczenia techniczne i programowe dla procedur, aplikacji, programów, baz danych i innych narzędzi programowych przetwarzających Dane osobowe opisane są w załączniku do Polityki.
5. W celu Zabezpieczenie Danych osobowych przed dostępem osób nieuprawnionych Administrator stosuje następującą politykę kluczy:
   a. klucze do pomieszczeń, budynku, szuflad i szaf (opis znajduje się w załączniku do niniejszej polityki)

§ 10.

1. Administrator prowadzi rejestr czynności przetwarzania, za które odpowiada. W rejestrze tym ujmowane są procesy, dla realizacji których niezbędne jest Przetwarzanie Danych osobowych. Rejestr zawiera co najmniej następujące informacje:
   a. nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów;
   b. cele przetwarzania;
   c. opis kategorii osób, których Dane dotyczą, oraz kategorii danych osobowych;
   d. kategorie odbiorców, którym Dane osobowe zostały lub zostaną ujawnione;
   e. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii Danych;
   f. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 Rozporządzenia,

   a także inne Dane umożliwiające przeprowadzenie wstępnej analizy ryzyka, ogólnej analizy ryzyka oraz oceny skutków dla ochrony Danych.
2. Rejestr czynności przetwarzania jest wykorzystywany przy realizacji obowiązków Administratora, o których mowa w § 8 Polityki.
3. Osobą odpowiedzialną za prowadzenie rejestru czynności przetwarzania jest Inspektor Ochrony Danych.
4. Rejestr czynności przetwarzania jest prowadzony w formie elektronicznej. Wzór rejestru stanowi załącznik do Polityki.
5. Rejestr czynności przetwarzania jest aktualizowany regularnie, nie rzadziej niż co 6 miesięcy.
6. Na żądanie organu nadzorczego Administrator udostępnia mu rejestr czynności przetwarzania.

IV. REALIZACJA ZASAD PRIVACY BY DESIGN I PRIVACY BY DEFAULT

§ 11.

1. Administrator w momencie ustalania sposobów przetwarzania Danych, jak i w trakcie samego procesu przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, tak aby Przetwarzanie było zgodne z wymogami Rozporządzenia i efektywnie chroniło prawa osób, których Dane dotyczą, przy uwzględnieniu charakteru, zakresu, kontekstu i celu przetwarzania danych oraz wynikającego z nich ryzyka dla praw i wolności osób fizycznych.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te Dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych Danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie Dane osobowe nie były udostępniane bez interwencji Danej osoby nieokreślonej liczbie osób fizycznych.

§ 12.

Administrator dokumentuje projektowanie ochrony danych osobowych, o którym mowa w § 11, za pomocą listy kontrolnej podsumowującej fazę projektowania ze wskazaniem przeanalizowanych rozwiązań w zakresie ochrony danych osobowych – wzór listy kontrolnej stanowi załącznik do Polityki.

V. OCENA SKUTKÓW DLA OCHRONY DANYCH

§ 13.

Jeżeli na podstawie analizy ryzyka przeprowadzonej zgodnie z § 7 Polityki wynika, że dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, zgodnie z postanowieniami działu V Polityki. W celu określenia, czy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator weryfikuje:

a. charakter,
b. zakres,
c. kontekst,
d. cele przetwarzania.

§ 14.

1. Ocena skutków dla ochrony danych, o której mowa w § 13, jest wymagana w szczególności w przypadku, gdy Przetwarzanie spełnia dwa lub więcej z poniższych kryteriów:
   a. Przetwarzanie wiąże się z oceną lub punktacją w tym profilowaniem i prognozowaniem w szczególności na podstawie aspektów dotyczących efektów pracy, sytuacji ekonomicznej,

zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której Dane dotyczą;

b. dochodzi do automatycznego podejmowania decyzji wywołującej wobec osoby, której Dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływającej;
c. Przetwarzanie obejmuje szczególnych kategorii Dane osobowe lub Dane o charakterze wysoce osobistym;
d. dochodzi do przetwarzania Danych na dużą skalę;
e. Przetwarzanie jest wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których Dane dotyczą, w tym Danych gromadzonych za pośrednictwem sieci lub ramach Systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie;
f. dochodzi do dopasowywania lub łączenia zbiorów Danych, w szczególności pochodzących z co najmniej dwóch różnych operacji przetwarzania Danych, przeprowadzonych w różnych celach lub przez różnych Administratorów Danych w sposób wykraczający poza uzasadnione oczekiwania osób, których Dane dotyczą;
g. Przetwarzanie obejmuje Dane osobowe osób wymagających szczególnej opieki, w tym np. dzieci lub pracowników;
h. następuje innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych;
i. samo Przetwarzanie uniemożliwia osobom, których Dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy.

2. Dla podobnych operacji przetwarzania Danych wiążących się z podobnym wysokim ryzykiem Administrator przeprowadza pojedynczą ocenę.
3. Administrator uwzględnia wykazy rodzajów operacji przetwarzania podlegających lub niepodlegających wymogowi dokonania oceny skutków dla ochrony Danych, ustanowione przez organ nadzorczy zgodnie z art. 35 ust. 4 i 5 Rozporządzenia.
4. W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony Danych, Administrator przeprowadza taką ocenę.

§ 15.

1. Ocena skutków dla ochrony Danych powinna rozpocząć się jak najwcześniej w fazie projektowania operacji przetwarzania. Jeżeli zachodzi taka potrzeba, w szczególności ze względu na zastosowane w projekcie środki techniczne lub organizacyjne, w miarę postępu procesu rozwoju lub w związku z istotną modyfikacją procesu, poszczególne etapy oceny należy powtórzyć.
2. Dokonując oceny skutków dla ochrony Danych, Administrator konsultuje się z Inspektorem Ochrony Danych, jeżeli został on powołany, a wyniki konsultacji i podjęte decyzje dokumentuje w ramach oceny skutków dla ochrony Danych.
3. Jeżeli dana operacja przetwarzania jest całkowicie lub częściowo realizowana przez Procesora, Administrator konsultuje się z Procesorem.
4. Jeżeli uzna to za właściwe, Administrator zasięga opinii osób, których Dane dotyczą, lub ich przedstawicieli. Jeżeli ostateczna opinia Administratora różni się od opinii osób, których Dane dotyczą, Administrator dokumentuje powody podjęcia bądź niepodjęcia decyzji. Administrator uzasadnia także niezasięgnięcia opinii osób, których Dane dotyczą, jeśli uzna je za niewłaściwe.
5. W stosownych przypadkach Administrator zasięga opinii niezależnych ekspertów z różnych dziedzin (np. prawników, informatyków, ekspertów z zakresu bezpieczeństwa).

6. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator dokonuje przeglądu, by stwierdzić, czy Przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

§ 16.

1. Administrator sporządza ocenę skutków dla ochrony danych na piśmie/ w formie elektronicznej.
2. Dokonując oceny skutków dla ochrony Danych Administrator uwzględnia i dokumentuje co najmniej:
   a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez Administratora;
   b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   c. ocenę ryzyka naruszenia praw lub wolności osób, których Dane dotyczą, o którym mowa w § 12; oraz
   d. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę Danych osobowych i wykazać przestrzeganie dotyczących jej przepisów, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których Dane dotyczą, i innych osób, których sprawa dotyczy;
   e. ocenę zgodności z kodeksami postępowania.
3. Ocena skutków dla ochrony Danych powinna uwzględniać certyfikację, znaki jakości oraz oznaczenia.

VI. POLITYKA ZARZĄDZANIA NARUSZENIAMI

§ 17.

1. Naruszenie ochrony Danych osobowych oznacza każde naruszenie bez względu na jego przyczynę prowadzące do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, a w szczególności:
   a. nieautoryzowany dostęp do Danych osobowych;
   b. utratę nośników zawierających Dane osobowe;
   c. nieautoryzowaną modyfikację lub zniszczenie Danych osobowych;
   d. bezpodstawne udostępnienie Danych osobowych;
   e. pozyskiwanie Danych osobowych z nielegalnych źródeł.
2. W przypadku stwierdzenia naruszenia zabezpieczenia Systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony Danych osobowych, każdy Członek personelu Administratora przerywa wykonywanie czynności związanych z Przetwarzaniem Danych osobowych i niezwłocznie informuje o tym fakcie Administratora lub bezpośredniego przełożonego, a następnie stosuje się do podjętych przez te osoby decyzji.
3. Powiadomienie o naruszeniu ochrony danych osobowych powinno obejmować:
   a. opis naruszenia ochrony Danych osobowych;
   b. określenie sytuacji, miejsca i czasu, w jakim stwierdzono naruszenie ochrony Danych osobowych;
   c. określenie wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia;

d. określenie znanych danej osobie sposobów zabezpieczenia Systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

4. Administrator lub inna upoważniona przez Administratora osoba podejmuje wszelkie działania mające na celu:
   a. minimalizację negatywnych skutków zdarzenia i ich późniejsze zupełne usunięcie;
   b. wyjaśnienie okoliczności zdarzenia;
   c. Zabezpieczenie dowodów zdarzenia;
   d. umożliwienie dalszego bezpiecznego przetwarzania Danych osobowych.
5. W celu realizacji procedury postępowania w przypadku naruszenia ochrony Danych osobowych Administrator lub wyznaczona przez Administratora osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   a. żądania wyjaśnień od Członków personelu;
   b. korzystania z pomocy konsultantów (w tym zewnętrznych podmiotów);
   c. nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania Danych osobowych.
6. Odmowa udzielenia przez pracownika wyjaśnień lub współpracy z Administratorem może być traktowana jako ciężkie naruszenie podstawowych obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1) Kodeksu pracy.
7. Administrator lub wyznaczona przez Administratora osoba, po stwierdzeniu naruszenia ochrony Danych osobowych, opracowuje raport końcowy, w którym przedstawia:
   a) okoliczności i charakter powstałego naruszenia, w tym:
      - kategorie i przybliżoną liczbę osób, których Danych dotyczy naruszenie,
      - kategorie i przybliżoną liczbę Danych osobowych, których dotyczy naruszenie,
      - możliwe konsekwencje powstałego naruszenia,
   b) wnioski i zalecenia ograniczające możliwość wystąpienia podobnego zdarzenia w przyszłości,
   c) opis podjętych działań zaradczych,

– wzór raportu stanowi załącznik do Polityki.

§ 18.

1. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Administrator bez zbędnej zwłoki – nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia – zgłasza je organowi nadzorczemu. Jeżeli zgłoszenie zostanie dokonane po upływie 72 godzin – należy dołączyć wyjaśnienie przyczyn opóźnienia - wzór zgłoszenia stanowi załącznik do Polityki.
2. Jeżeli w zakreślonym wyżej czasie Administrator nie jest w stanie zgromadzić i przekazać organowi nadzorczemu wszystkich wymaganych informacji – może ich udzielać sukcesywnie – bez zbędnej zwłoki.
3. Zgłoszenie naruszenia ochrony Danych osobowych (opisane w ust. 1) nie jest wymagane, jeśli jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Za dokonanie oceny istnienia lub nieistnienia powyższego ryzyka odpowiada Administrator.
4. W sytuacji, kiedy naruszenie ochrony Danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – Administrator bez zbędnej zwłoki zawiadamia także osobę, której Dane dotyczą, o wystąpieniu naruszenia. Wzór zawiadomienia stanowi załącznik do Polityki.
5. W zawiadomieniu, o którym mowa w pkt. 4, umieszcza się informacje w zakresie:

a) imienia i nazwiska oraz danych kontaktowych Inspektora Ochrony Danych osobowych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji nt. naruszenia,
b) konsekwencji naruszenia ochrony Danych osobowych, które mogą pojawić się dla osoby, której Dane dotyczą w związku z zaistnieniem naruszenia,
c) środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach, także środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

6. Zawiadomienie, o którym mowa w pkt. 4, nie jest wymagane w następujących przypadkach:
   a) zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony, które zostały zastosowane do Danych osobowych, których dotyczy naruszenie – w szczególności środki takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych Danych;
   b) następnie zostały zastosowane środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której Dane dotyczą;
   c) wymagałoby to niewspółmiernie dużego wysiłku – w takim wypadku należy wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby, których Dane dotyczą, zostają poinformowane w równie skuteczny sposób.

VII. ZASADY DOPUSZCZANIA OSÓB WEWNĄTRZ ORGANIZACJI DO PRZETWARZANIA DANYCH

§ 19.

1. Do przetwarzania Danych osobowych mogą zostać dopuszczone wyłącznie osoby przeszkolone, którym Administrator nadał na piśmie lub w formie dokumentowej odpowiednie upoważnienie do przetwarzania Danych osobowych – wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik do Polityki.
2. Z zastrzeżeniem ust. 3 niniejszego paragrafu, każdy dopuszczony do przetwarzania Danych osobowych pracownik po odbyciu szkolenia oraz po otrzymaniu upoważnienia do przetwarzania Danych osobowych składa na piśmie oświadczenie o poufności, którego treść uzależniona jest od zakresu obowiązków danego pracownika– wzory oświadczeń o poufności stanowią załączniki do Polityki.
3. W przypadku, gdy do przetwarzania Danych osobowych dopuszczona jest osoba świadcząca pracę w ramach cywilnoprawnej formy zatrudnienia lub osoba prowadząca indywidualną działalność gospodarczą, stale współpracująca z Administratorem, z osobą taką, po nadaniu jej na piśmie lub w formie dokumentowej odpowiedniego upoważnienia do przetwarzania Danych osobowych, zawierana jest umowa o poufności – wzór umowy o poufności stanowi załącznik do Polityki.
4. W przypadku, gdy podmiot zewnętrzny deleguje swoich pracowników lub osoby świadczące u niego pracę w ramach cywilnoprawnych form zatrudnienia do świadczenia usług pod kontrolą i na fizycznym obszarze przetwarzania danych Administratora oraz jeżeli nie zachodzi relacja uzasadniająca zawarcie umowy powierzenia, wyżej wymienionym pracownikom lub osobom nadawane jest na piśmie lub w formie dokumentowej upoważnienie do przetwarzania Danych osobowych i odbierane jest od nich pisemne oświadczenie o poufności – wzór oświadczenia o poufności stanowi załącznik do Polityki.

5. Administrator zapewnia, by każda osoba fizyczna działająca z jego upoważnienia, która ma dostęp do Danych osobowych, przetwarzała je wyłącznie na polecenie Administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

§ 20.

6. Upoważnienie, o którym mowa w § 19 ustępie 1, musi być aktualne. W przypadku przedłużającej się nieobecności osoby upoważnionej lub zaprzestania wykonywania przez nią części lub wszystkich obowiązków, uzasadniających potrzebę upoważnienia jej do przetwarzania Danych osobowych, upoważnienie musi zostać w odpowiednim zakresie odwołane – wzór odwołania upoważnienia stanowi załącznik do Polityki.
7. Utrata uprawnień do przetwarzania Danych osobowych objętych upoważnieniem może nastąpić w szczególności w przypadku:
   1) odwołania upoważnienia przez Administratora bez podania przyczyny;
   2) rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z Administratorem;
   3) zmiany stanowiska pracy osoby upoważnionej u Administratora na stanowisko nieuzasadniające konieczności posiadania dostępu do zbiorów Danych osobowych, jeżeli nowy zakres czynności nie wykazuje obowiązków służbowych związanych z Przetwarzaniem Danych osobowych;
   4) umyślnego naruszenia przez osobę upoważnioną zasad ochrony Danych osobowych określonych w Rozporządzeniu, ustawie, Polityce.
8. W przypadku utraty uprawnień do przetwarzania Danych osobowych, Administrator niezwłocznie odwołuje upoważnienie do przetwarzania Danych osobowych oraz dokonuje zmian w ewidencji osób upoważnionych do przetwarzania Danych osobowych.

§ 21.

Administrator prowadzi ewidencję osób upoważnionych do przetwarzania Danych osobowych w wersji papierowej/elektronicznej odnotowując informacje o wszystkich wydanych upoważnieniach oraz adnotacje o ich odwołaniu – wzór ewidencji osób upoważnionych stanowi załącznik do Polityki.

§ 22.

1. Dla wszystkich Użytkowników stosowane są uprawnienia do zasobów i zbiorów wedle zasady niezbędnego minimum potrzebnego do wykonywania obowiązków pracowniczych lub służbowych.
2. ASI nadaje określone uprawnienia dostępu do Systemów informatycznych w porozumieniu z Administratorem.
3. ASI nadaje, zmienia lub odwołuje uprawnienia w Systemie informatycznym zgodnie z dyspozycjami Administratora.
4. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania Danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania Danych osobowych nadane przez Administratora.
5. Użytkownicy powinni pracować na kontach zwykłych Użytkowników. Praca na kontach administracyjnych jest dopuszczalna tylko dla ASI oraz upoważnionych przez niego osób.

6. W przypadku wycofania uprawnień Użytkownika do Systemu informatycznego, w którym przetwarzane są Dane osobowe, ASI niezwłocznie blokuje konto Użytkownika i informuje o tym fakcie Administratora i Inspektora Ochrony Danych.
7. Identyfikator nowego konta w Systemie informatycznym nadany zgodnie z wnioskiem przez ASI musi być unikalny.
8. Za kontrolę aktualności kont Użytkowników wraz z uprawnieniami im nadanymi odpowiedzialny jest ASI.
9. Osobą zastępującą ASI w sytuacjach awaryjnych jest pracownik działu IT wskazany przez ASI.

§ 23.

1. Każdy Członek personelu przed nadaniem mu upoważnienia do przetwarzania Danych osobowych zostaje przeszkolony z zakresu ochrony Danych osobowych przez Inspektora Ochrony Danych/ osobę wyznaczoną przez Administratora, przy czym szkolenie to zostaje zakończone podpisaniem przez osobę szkoloną oświadczenia o wzięciu udziału w szkoleniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony Danych osobowych.
2. W przypadku zmian przepisów dotyczących ochrony Danych osobowych lub zasad przetwarzania i ochrony Danych osobowych u Administratora Inspektor Ochrony Danych/ osoba wyznaczona przez Administratora niezwłocznie organizuje szkolenie dla Członków personelu.
3. W celu przeprowadzenia szkolenia Inspektor Ochrony Danych/ osoba wyznaczona przez Administratora może korzystać z pomocy wyspecjalizowanych podmiotów zewnętrznych posiadających odpowiednio wysoki poziom wiedzy i kwalifikacje do prowadzenia szkoleń z zakresu ochrony danych osobowych.
4. Inspektor Ochrony Danych/ osoba wyznaczona przez Administratora prowadzi dokumentację dotyczącą przeprowadzonych szkoleń, w tym sporządza po przeprowadzeniu każdego szkolenia listę osób, które wzięły w nim udział.
5. Inspektor Ochrony Danych co najmniej raz w roku powinien uczestniczyć w szkoleniach zewnętrznych związanych z ochroną danych osobowych.

VIII. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

§ 24.

1. Przetwarzanie Danych przez Procesora, z którego usług korzysta Administrator, odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i Administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj Danych osobowych oraz kategorie osób, których Dane dotyczą, obowiązki i prawa Administratora.
2. Przetwarzanie Danych przez Procesora, z którego usług korzysta Administrator, nie powoduje zmiany właściwego Administratora.

§ 25.

1. Dokonując wyboru Procesora Administrator korzysta z usług tylko takich Procesorów, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby Przetwarzanie Danych spełniało wymogi przepisów i chroniło prawa osób, których Dane dotyczą. Administrator bierze pod uwagę w szczególności fachową wiedzę, wiarygodność i zasoby Procesora.
2. Wystarczające gwarancje, o których mowa w ust. 1, Procesor może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 Rozporządzenia.(brak kodeksu postępowania dla firmy)
3. Weryfikacji zapewniania przez Procesora gwarancji, o których mowa w ust. 1, Administrator dokonuje z wykorzystaniem z listy kontrolnej, której wzór stanowi załącznik do Polityki.

§ 26.

Jeżeli inny podmiot polecił Administratorowi Przetwarzanie Danych osobowych w jego imieniu, Administrator, działając jako podmiot przetwarzający, zobowiązany jest:

a. przetwarzać Dane osobowe wyłącznie na udokumentowane polecenie powierzającego – co dotyczy też przekazywania Danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje powierzającego Dane o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
b. zapewnić, by osoby upoważnione do przetwarzania Danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c. podejmować wszelkie środki dotyczące bezpieczeństwa przetwarzania, wymagane na mocy art. 32 Rozporządzenia;
d. przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 Rozporządzenia;
e. uwzględniając charakter przetwarzania, w miarę możliwości pomagać powierzającemu Dane poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której Dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia;
f. uwzględniając charakter przetwarzania oraz dostępne informacje, pomagać powierzającemu Dane wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia;
g. po zakończeniu świadczenia usług związanych z Przetwarzaniem - zależnie od decyzji powierzającego – usunąć lub zwrócić powierzającemu wszelkie Dane osobowe oraz usunąć wszelkie istniejące kopie tych Danych, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie Danych osobowych;
h. udostępniać powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym ustępie oraz umożliwić powierzającemu lub

upoważnionej przez niego osobie przeprowadzenie audytów, w tym inspekcji, i przyczyniać się do nich;

i. prowadzić rejestr kategorii czynności przetwarzania, którego wzór stanowi załącznik do Polityki.

§ 27.

1. Umowa, na podstawie której odbywa się Przetwarzanie Danych (określa załącznik do niniejszej Polityki)
2. Umowa może zostać zawarta w formie pisemnej lub w formie dokumentowej.
3. Administrator odnotowuje w rejestrze czynności przetwarzania wszystkie umowy powierzenia przetwarzania.

§ 28.

1. Administrator w miarę potrzeby przeprowadzi audyt Procesora w zakresie zgodności wykonywania przez niego czynności przetwarzania Danych osobowych z postanowieniami umowy, o której mowa w § 27 Polityki, oraz obowiązującymi przepisami o ochronie Danych, w szczególności w celu sprawdzenia wykonywania przez Procesora ciążących na nim obowiązków.
2. Zasady przeprowadzenia audytu określa umowa, o której mowa w § 27 Polityki.
3. Administrator przekaże Procesorowi, po przeprowadzonym audycie, pisemnych zaleceń i wytycznych wraz z terminem ich realizacji, dotyczących w szczególności zabezpieczenia danych osobowych pod względem technicznym i organizacyjnym oraz sposobu wykonywania czynności ich przetwarzania. Administrator może zrezygnować z przeprowadzenia audytu Procesora jedynie w wyjątkowych przypadkach, gdy Powierzenie przetwarzania ma charakter bagatelny.

IX. ZASADY UJAWNIANIA DANYCH ODBIORCOM INNYM NIŻ PROCESOROWI

§ 29.

1. Ujawnianie Danych osobowych odbiorcom innym niż Procesorowi dopuszczalne jest tylko w przypadku spełnienia jednej z przesłanek przetwarzania Danych osobowych określonych w § 4 Polityki.
2. Ujawnianie Danych osobowych może nastąpić tylko po uprzednim przedstawieniu wniosku o ich ujawnienie. Wniosek powinien mieć formę pisemną lub dokumentową i zawierać:
    a. oznaczenie wnioskodawcy;
    b. wskazanie podstaw legalizacyjnych uzasadniających żądanie ujawnienia;
    c. określenie rodzaju i zakresu żądanych informacji oraz formy ich przekazania lub udostępnienia;
    d. wskazanie imienia, nazwiska i stanowiska osoby upoważnionej do otrzymania Danych osobowych lub zapoznania się z ich treścią.
3. Ujawnianie Danych osobowych na podstawie ustnego wniosku zawierającego wszystkie cztery elementy określone w ust. 2 może nastąpić wyłącznie, gdy zachodzi konieczność niezwłocznego działania.

§ 30.

1. Osoba udostępniająca Dane osobowe jest obowiązana zażądać od osoby uprawnionej pokwitowania ujawnienia danych, zawierającego informacje przekazane na podstawie wniosku złożonego na piśmie lub w formie dokumentowej albo potwierdzenie faktu uzyskania wglądu w treść informacji.
2. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie otrzymania informacji. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
3. Jeśli osoba uprawniona pouczyła osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze czynności przetwarzania niezależnie od odnotowania faktu udostępnienia informacji.
4. W celu zapewnienia kontroli nad tym, jakie Dane osobowe, kiedy i przez kogo oraz komu zostały przekazane, Administrator odnotowuje ujawnienie Danych w rejestrze czynności przetwarzania.

X. ZAKOŃCZENIE PRZETWARZANIA - POLITYKI RETENCYJNE

§ 31.

1. Dane osobowe są przechowywane przez okres nie dłuższy niż jest to niezbędne do celów, w których Dane te są przetwarzane. Okresy przechowywania poszczególnych kategorii Danych osobowych określa załącznik do Polityki.
2. Po zakończeniu przetwarzania Danych osobowych Administrator zobowiązany jest do niezwłocznego usunięcia Danych osobowych i wszelkich istniejących ich kopii, zarówno elektronicznych, jak i papierowych.
3. Z usunięcia Danych osobowych i ich kopii Administrator sporządza protokół.

XI. PRAWA PODMIOTU DANYCH

§ 32.

W celu realizacji swoich praw, podmiot danych kontaktuje się z Inspektorem Ochrony Danych, jeżeli został on powołany za pomocą adresu e-mail: ……. lub tel:.....

§ 33.

1. Przetwarzanie Danych osobowych przez Administratora powinno być zgodne z prawem i rzetelne. Dla osób, których Dane dotyczą, powinno być przejrzyste, że dotyczące ich Dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te Dane osobowe są lub będą przetwarzane. Wszelkie informacje i wszelkie komunikaty związane z Przetwarzaniem tych Danych osobowych powinny być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których Dane dotyczą, o tożsamości Administratora i celach przetwarzania oraz innych informacji

mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych Danych osobowych ich dotyczących.

2. Osobom, których Dane dotyczą, należy uświadamiać ryzyka, zasady, zabezpieczenia i prawa związane z Przetwarzaniem Danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim Przetwarzaniem. W szczególności konkretne cele przetwarzania Danych osobowych przez Administratora powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.

§ 34.

1. Jeżeli Dane osobowe osoby, której Dane dotyczą, zbierane są od tej osoby, Administrator podczas pozyskiwania Danych osobowych podaje jej informacje określone w § 13 ust. 1, 2 i 3 Rozporządzenia, chyba że ta osoba dysponuje już tymi informacjami.
2. Jeżeli Danych osobowych nie pozyskano od osoby, której Dane dotyczą, Administrator podaje jej informacje określone w § 14 ust. 1, 2 i 4 Rozporządzenia, chyba że:
   a. ta osoba dysponuje już tymi informacjami;
   b. udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
   c. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której Dane dotyczą; lub
   d. Dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.
3. Informacje, o których mowa w ust. 2, Administrator podaje:
   a. w rozsądnym terminie po pozyskaniu Danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania Danych osobowych;
   b. jeżeli Dane osobowe mają być stosowane do komunikacji z osobą, której Dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której Dane dotyczą; lub
   c. jeżeli planuje się ujawnić Dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.
4. Wzory klauzul informacyjnych stosowanych w przypadkach, o których mowa w ust. 1 i 2, stanowią załączniki do Polityki.

§ 35.

1. Jeżeli podstawą przetwarzania Danych osobowych jest Zgoda osoby, której Dane dotyczą, Administrator musi być w stanie wykazać, że osoba, której Dane dotyczą, wyraziła zgodę na Przetwarzanie swoich Danych osobowych.(zasada rozliczalności)
2. Zgoda powinna być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, którym osoba, której Dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na Przetwarzanie dotyczących jej Danych osobowych w konkretnym celu. Na różne cele przetwarzania powinna być odbierana osobna Zgoda.

3. Jeżeli osoba, której Dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, 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. Wzór zapytania o zgodę składanego w formie pisemnej/ elektronicznej/ telefonicznej/ przy osobistym kontakcie z osobą, której Dane dotyczą, stanowi załącznik do Polityki.
4. Administrator umożliwia osobie, której Dane dotyczą, wycofanie zgody w dowolnym momencie w taki sam sposób, w jaki nastąpiło jej wyrażenie. Administrator w jasny i przejrzysty sposób informuje osobę, której Dane dotyczą, o możliwości wycofania zgody. W przypadku wycofania zgody Administrator niezwłocznie zaprzestaje przetwarzania Danych tej osoby.
5. Wyrażenie zgody na Przetwarzanie Danych nie może stanowić warunku zawarcia umowy lub świadczenia usługi.
6. W przypadku planu zmiany celu przetwarzania Danych, Administrator ponownie zwraca się do osoby, której Dane dotyczą, o zgodę na Przetwarzanie jej Danych co do zmienianego celu.

§ 36.

1. Administrator umożliwia osobie, której Dane dotyczą, uzyskanie potwierdzenia, czy przetwarzane są Dane osobowe jej dotyczące, a jeżeli ma to miejsce, również uzyskanie dostępu do nich i informacji określonych w § 15 ust. 1 i 2 Rozporządzenia.
2. Administrator dostarcza osobie, której Dane dotyczą, kopię Danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której Dane dotyczą, Administrator pobiera opłatę w wysokości 40 zł, które wynikają z kosztów administracyjnych. Jeżeli osoba, której Dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w korespondencji mailowej.

§ 37.

1. Administrator dokonuje sprostowania nieprawidłowych Danych na żądanie osoby, której Dane dotyczą, niezwłocznie po otrzymaniu takiego żądania.
2. Administrator uzupełnia niekompletne Dane osobowe na żądanie osoby, której Dane dotyczą, niezwłocznie po otrzymaniu takiego żądania. Administrator odmawia uzupełnienia Danych osobowych, gdy jest ono niezgodne z celami przetwarzania.
3. Administrator weryfikuje merytoryczną poprawność Danych osobowych wskazanych w żądaniu sprostowania lub uzupełnienia Danych.
4. Administrator informuje o sprostowaniu, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

§ 38.

1. Na żądanie osoby, której Dane dotyczą, Administrator usuwa dotyczące je Dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
    a. Dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b. osoba, której Dane dotyczą, cofnęła zgodę, na której opiera się Przetwarzanie, i nie ma innej podstawy prawnej przetwarzania;
c. osoba, której Dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której Dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 Rozporządzenia wobec przetwarzania;
d. Dane osobowe były przetwarzane niezgodnie z prawem;
e. Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;
f. Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego,

2. Jeżeli Administrator upublicznił Dane osobowe, które zgodnie z ust. 1 ma obowiązek usunąć, to - biorąc pod uwagę dostępną technologię i koszt realizacji - podejmuje rozsądne działania, w tym środki techniczne, by poinformować Administratorów przetwarzających te Dane osobowe, że osoba, której Dane dotyczą, żąda, by Administratorzy ci usunęli wszelkie łącza do tych Danych, kopie tych Danych osobowych lub ich replikacje. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
3. Administrator może odmówić usunięcia Danych w zakresie, w jakim jest ono niezbędne:
   a. do korzystania z prawa do wolności wypowiedzi i informacji;
   b. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
   c. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, o ile prawdopodobne jest, że usunięcie Danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
   d. do ustalenia, dochodzenia lub obrony roszczeń.
4. Administrator zaniecha przetwarzania Danych osobowych niezwłocznie po otrzymaniu sprzeciwu osoby, której Dane dotyczą, jeżeli Przetwarzanie było niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią. Administrator może nie uwzględnić sprzeciwu, jeżeli wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której Dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
5. Żądanie usunięcia danych lub sprzeciw osoba, której Dane dotyczą, może złożyć w formie pisemnej, elektronicznej, w tym za pośrednictwem strony internetowej Administratora, telefonicznie lub ustnie do protokołu w siedzibie Administratora.

§ 39.

1. Jeżeli Przetwarzanie odbywa się na podstawie zgody osoby, której Dane dotyczą, i w sposób zautomatyzowany, Administrator umożliwia osobom, których Dane dotyczą, otrzymanie kopii ich

Danych osobowych w formie elektronicznej, w formacie *.xml, *.json, *.csv lub innym powszechnie używanym, ustrukturyzowanym formacie, nadającym się do odczytu maszynowego, umożliwiającym tej osobie przesłanie Danych do innego dostawcy usług, odczytanie Danych w sposób automatyczny przez innego dostawcę i korzystanie z Danych w ramach usług innego dostawcy.

2. O ile jest to technicznie możliwe, na żądanie osoby, której Dane dotyczą, Administrator przesyła Dane osobowe bezpośrednio innemu Administratorowi.
3. Administrator może odmówić udostępnienia kopii Danych zgodnie z ust. 1, jeżeli mogłoby ono niekorzystnie wpływać na prawa i wolności innych.

§ 40.

1. Administrator ogranicza Przetwarzanie Danych na żądanie osoby, której Dane dotyczą, w następujących przypadkach:
    a. osoba, której Dane dotyczą, kwestionuje prawidłowość Danych osobowych - na okres pozwalający Administratorowi sprawdzić prawidłowość tych Danych;
    b. Przetwarzanie jest niezgodne z prawem, a osoba, której Dane dotyczą, sprzeciwia się usunięciu Danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
    c. Administrator nie potrzebuje już Danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której Dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
    d. osoba, której Dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której Dane dotyczą.
2. Administrator przechowuje Dane, których Przetwarzanie zostało ograniczone zgodnie z ust. 1, a w pozostałym zakresie przetwarza je wyłącznie:
    a. za zgodą osoby, której Dane dotyczą, lub
    b. w celu ustalenia, dochodzenia lub obrony roszczeń, lub
    c. w celu ochrony praw innej osoby fizycznej lub prawnej, lub
    d. z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3. Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której Dane dotyczą, która żądała ograniczenia.
4. Administrator informuje o ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

§ 41.

1. Administrator dopuszcza podejmowanie decyzji, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołują skutki prawne wobec osoby, której Dane dotyczą, lub w podobny sposób istotnie na nią wpływają, wyłącznie jeżeli taka decyzja:
    a. jest niezbędna do zawarcia lub wykonania umowy między osobą, której Dane dotyczą, a Administratorem;

b. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której Dane dotyczą; lub
c. opiera się na wyraźnej zgodzie osoby, której Dane dotyczą.

2. W przypadkach, o których mowa w ust. 1 lit. a i c, na żądanie osoby, której Dane dotyczą, Administrator zapewni weryfikację interwencję ludzką. Administrator umożliwi osobie, której Dane dotyczą, wyrażenie własnego stanowiska i zakwestionowanie decyzji podjętej w sposób określony w ust. 1.
3. Decyzje, o których mowa w ust. 2, nie mogą opierać się na Szczególnych kategoriach Danych osobowych, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) Rozporządzenia i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której Dane dotyczą.

XII. IOD - INSPEKTOR OCHRONY DANYCH

§ 42.

Administrator wyznacza Inspektora Ochrony Danych, gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność Administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i Systematycznego monitorowania osób, których Dane dotyczą, na dużą skalę; lub

c) główna działalność Administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę Szczególnych kategorii Danych osobowych lub Danych osobowych dotyczących wyroków i naruszeń prawa.

W pozostałych przypadkach wyznaczenie Inspektora Ochrony Danych jest fakultatywne.

§ 43.

1. Do pełnienia funkcji Inspektora Ochrony Danych może zostać wyznaczona wyłącznie osoba spełniająca warunki określone w art. 37 ust. 5 Rozporządzenia, tj. posiadająca kwalifikacje zawodowe, a w szczególności fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętność wypełnienia powierzonych mu zadań.
2. Formalne wyznaczenie do pełnienia funkcji Inspektora Ochrony Danych następuje na podstawie dokumentu wyznaczenia Inspektora Ochrony Danych, którego wzór stanowi załącznik do Polityki.
3. Administrator publikuje Dane kontaktowe Inspektora Ochrony Danych i zawiadamia o nich organ nadzorczy.

§ 44.

1. Administrator zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony Danych osobowych.

2. Administrator wspiera Inspektora Ochrony Danych w wypełnianiu przez niego zadań, o których mowa w § 45 zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do Danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
3. Inspektor Ochrony Danych nie otrzymuje instrukcji dotyczących wykonywania swoich zadań, nie jest odwoływany ani karany za wypełnianie swoich zadań.
4. Inspektor Ochrony Danych podlega bezpośrednio najwyższemu kierownictwu Administratora.
5. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
6. Jeżeli Inspektor Ochrony Danych wykonuje inne zadania i obowiązki, Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

§ 45.

1. Do zadań Inspektora Ochrony Danych należą w szczególności:
   a. informowanie Administratora, współpracujących z nim Procesorów oraz pracowników, którzy przetwarzają Dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b. monitorowanie przestrzegania Rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie Danych oraz Polityki, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony Danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;
   d. współpraca z organem nadzorczym;
   e. 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;
   f. kontakt z osobami, których Dane dotyczą, we wszystkich sprawach związanych z Przetwarzaniem ich Danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia;
   g. przygotowywanie dla Administratora, co najmniej raz w roku, pisemnego sprawozdania ze swojej działalności;
   h. prowadzenie i aktualizowanie dokumentacji dotyczącej ochrony Danych osobowych u Administratora, w szczególności rejestru czynności przetwarzania;
   i. poddawaniu, co najmniej raz w roku, przeglądowi Polityki pod kątem jej aktualności oraz zgodności deklarowanego w niej stanu z prawem;
   j. nadzorowanie Powierzania przetwarzania Danych osobowych innym podmiotom, w szczególności nadzorowanie spełnienia wymagań Rozporządzenia przez Procesora;
   k. nadzorowanie udostępniania Danych osobowych;
   l. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony Danych osobowych;
   m. podejmowanie, wspólnie z Administratorem i ASI, odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania Danych osobowych;

n. przygotowywaniu materiałów szkoleniowych z zakresu ochrony Danych osobowych i prowadzeniu cyklicznych szkoleń osób upoważnianych do przetwarzania Danych osobowych lub współpraca w tym zakresie z wyspecjalizowanym podmiotem zewnętrznym;
o. wyznaczanie w formie pisemnej, w porozumieniu z Administratorem, swojego zastępcy na czas swojej nieobecności.

2. W celu prawidłowego wykonywania powierzonych zadań, Inspektor Ochrony Danych jest uprawniony do:
   a. wstępu do pomieszczeń, w których zlokalizowane są Dane osobowe i przeprowadzenia wszystkich niezbędnych czynności kontrolnych w celu oceny zgodności przetwarzania danych z Rozporządzeniem, ustawą i Polityką;
   b. żądania od członków personelu, w tym od osób upoważnionych, złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego dotyczącego przetwarzania Danych i ich zabezpieczenia,
   c. żądania udostępnienia do kontroli zgodności przetwarzania Danych z przepisami o ochronie danych dokumentacji, urządzeń, nośników oraz Systemów informatycznych służących do przetwarzania Danych osobowych u Administratora,
   d. występowania w porozumieniu z Administratorem do Procesora o wyjaśnienia i informacje dotyczące przetwarzania powierzonych Danych,
   e. prowadzenia działań kontrolnych u Procesora w zakresie zgodności przetwarzania powierzonych Danych z przepisami o ochronie Danych i z umową o której mowa w art. 28 Rozporządzenia, w tym także żądania okazania dokumentów,
   f. wyznaczania, rekomendowania i egzekwowania od członków personelu wykonania zadań związanych z ochroną Danych osobowych;
   g. wydawania członkom personelu wiążących poleceń dotyczących przetwarzania i ochrony Danych osobowych u Administratora.
3. Inspektor Ochrony Danych nadzoruje przestrzeganie zasad przetwarzania i ochrony Danych osobowych, zwłaszcza poprzez:
   a. prowadzenie sprawdzeń planowych i doraźnych oraz dokumentowanie czynności kontrolnych,
   b. coroczne opracowywanie planu sprawdzeń w zakresie ochrony Danych osobowych – plan kontroli obejmuje rok kalendarzowy;
   c. przeprowadzanie kontroli Systemu informatycznego (zleca ASI);
   d. przeprowadzanie kontroli zabezpieczeń fizycznych;
   e. pisemne informowanie Administratora o wynikach przeprowadzonych kontroli.
4. Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

XIII. ODPOWIEDZIALNOŚĆ OSÓB PRZETWARZAJĄCYCH DANE W RAMACH ORGANIZACJI

§ 46.

1. Nieprzestrzeganie zasad określonych w Polityce stanowi w przypadku pracowników naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności pracowniczej określonej w Kodeksie pracy.
2. Jeżeli skutkiem działania określonego w ustępie powyżej jest szkoda, Członek personelu:
    a. będący pracownikiem ponosi odpowiedzialność materialną na zasadach określonych w Kodeksie pracy,
    b. niebędący pracownikiem ponosi odpowiedzialność na zasadach ogólnych Kodeksu cywilnego.

XIV. FIZYCZNE OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH

§ 47.

1. Siedziba firmy Kyrylo Radionov mieści przy ul. Gagarina 19/332 w Toruniu.

XV. POSTANOWIENIA KOŃCOWE

§ 48.

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w jakiejkolwiek formie.
2. Członek personelu zobowiązany jest złożyć oświadczenie o tym, iż został zapoznany z przepisami Rozporządzenia i ustawy oraz postanowieniami Polityki wdrożonej do stosowania u Administratora, a także o zobowiązaniu się do ich przestrzegania.
3. Oświadczenie, o którym mowa w ust. 2 powyżej, złożone przez Użytkownika będącego pracownikiem przechowywane jest jego w aktach osobowych.
4. Wszyscy upoważnieni do przetwarzania danych osobowych zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
5. W sprawach nieuregulowanych w Polityce zastosowanie mają przepisy Rozporządzenia i ustawy.

Załączniki:
1. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.
2. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
3. *Lista kontrolna.* Jak zgodnie ze wskazówkami GIODO powierzyć przetwarzanie danych osobowych.
4. *Lista kontrolna:* Jak postąpić w przypadku naruszenia ochrony danych osobowych.
5. Oświadczenie o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych.
6. *Wzór* - Klauzuli informacyjnej art. 13 RODO
7. *Wzór* - Klauzuli informacyjnej stosowanej – w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą. (art. 14 RODO)
8. *Wzór* - Klauzuli zgody na przetwarzanie danych osobowych zgodnej z RODO.
9. *Wzór* - Raportu z naruszenia ochrony danych.
10. *Wzór* - Rejestru czynności przetwarzania danych osobowych.
11. *Wzór* - Rejestru naruszeń ochrony danych osobowych.
12. *Wzór* - Umowy powierzenia przetwarzania danych osobowych.
13. *Wzór* - Klauzula dotycząca kontroli wykonywania umowy przez procesora.
14. *Wzór* - Klauzula informująca o konkretnym podwykonawcy.
15. *Wzór* - Klauzula odpowiedzialności w umowie podpowierzenia.
16. *Wzór* - Klauzula umożliwiająca podpowierzenie danych osobowych.
17. *Wzór* - Upoważnienia do przetwarzania danych osobowych.
18. *Wzór* - Zarządzenia w sprawie wyznaczenia Inspektora Ochrony Danych.
19. *Wzór* - Zgłoszenia naruszenia ochrony danych osobowych.
20. *Wzór* - Zawiadomienia o naruszeniu ochrony danych osobowych kierowanego do osoby, której dane dotyczą.
21. Rejestr czynności przetwarzania (Polityki retencyjne).
22. *Wzór* - Klauzula art.13 wersja rozszerzona
23. Polityka monitoringu wizyjnego.
24. Wzór umowy powierzenia przetwarzania danych osobowych-DWUSTRONNA