WSTĘP

1.1 INFORMACJE OGÓLNE

1. Wskazanie Administratora Danych, który wdraża Politykę Bezpieczeństwa. Justyna Kaleta prowadząca działalność gospodarczą pod firmą Centrum Szkółkarskie „Justyna" Justyna Kaleta, ul. Trakt Św. Wojciecha 291, 80-018 Gdańsk, NIP 5831005468

2. Wyjaśnienie celu wprowadzania dokumentu.

   Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Administratora Danych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE)2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – Dz. Urz. UE L 119, s. 1 (dalej RODO), ustawą o ochronie danych osobowych oraz z rozporządzeniami wykonawczymi do ustawy.

3. Wskazanie podstaw prawnych.

   Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

   a. rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – Dz.Urz. UE L 119, s 1

   b. ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2018 r., poz. 1000).

1.2 ZAKRES INFROMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Niniejszy dokument zatytułowany „Polityka ochrony danych osobowych" (dalej: Polityka) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w (zwanym dalej: Administratorem). Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s.1).

1. Polityka zawiera:
   - **a.** opis zasad ochrony danych obowiązujących u Administratora,
   - **b.** wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe
   - **c.** określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
   - **d.** odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).
2. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator Danych – Justyna Kaleta prowadząca działalność gospodarczą pod firmą Centrum Szkółkarskie „Justyna"

   Za nadzór i monitorowanie przestrzegania Polityki odpowiadają:

   Administrator Danych.

Administrator powinien też zapewnić zgodność postępowania kontrahentów Administratora z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Administratora.

1.3 WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

SKRÓTY I DEFINICJE:

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1).

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

Dane szczególnych kategorii oznaczają dane wymienione w art.9 ust.1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 16. roku życia.

Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Podmiot przetwarzający oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych (np. Usługodawca IT, zewnętrzna księgowość).

Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

IOD lub Inspektor oznacza Inspektora Ochrony Danych Osobowych.

RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Administrator oznacza Justynę Kaleta

1.4 OCHRONA DANYCH OSOBOWYCH W SPÓŁCE – ZASADY OGÓLNE

Filary ochrony danych osobowych w Przedsiębiorstwie:

(1) Legalność – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.

(3) Prawa jednostki – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) Rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili moc wykazać zgodność.

Zasady ochrony danych

Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

(1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

(2) rzetelnie i uczciwie (rzetelność);

(3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

(4) w konkretnych celach i nie „na zapas” (minimalizacja);

(5) nie więcej niż potrzeba (adekwatność);

(6) z dbałością o prawidłowość danych (prawidłowość);

(7) nie dłużej niż potrzeba (czasowość);

(8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

System ochrony danych

System ochrony danych osobowych u Administratora składa się z następujących **elementów**:

1. Inwentaryzacja danych.

Administrator dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych szczególnych kategorii i danych karnych;

b) przypadków przetwarzania danych osób, których Administrator nie identyfikuje (dane niezidentyfikowane/UFO);

c) przypadków przetwarzania danych dzieci;

d) profilowania;

e) współadministrowania danymi.

2. Rejestr.

Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych

3. Podstawy prawne.

Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

4. Obsługa praw jednostki.

Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) obowiązki informacyjne Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;

b) możliwość wykonania żądań. Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;

c) obsługa żądań. Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane;
d) zawiadamianie o naruszeniach. Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5. Minimalizacja.
Administrator posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
a) zasady zarządzania adekwatnością danych;
b) zasady reglamentacji i zarządzania dostępem do danych;
c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

6. Bezpieczeństwo.
Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;
b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
c) dostosowuje środki ochrony danych do ustalonego ryzyka;
d) posiada system zarządzania bezpieczeństwem informacji;
e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

7. Przetwarzający.
Administrator posiada zasady doboru przetwarzających dane na rzecz Administratora, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.
8. Eksport danych.
Administrator posiada zasady weryfikacji, czy Administrator nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub do

organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

9. *Privacy by design*.

Administrator zarządza zmianami wpływającymi na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10. Przetwarzanie transgraniczne.

Administrator posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1 INFORMACJE OGÓLNE

1. Punkt ten wskazuje osoby odpowiedzialne za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki Bezpieczeństwa oraz załączników do niej.
2. Administrator Danych: Justyna Kaleta

2.2 ADMINISTRATOR DANYCH

1. Podrozdział wskazuje, kto jest Administratorem Danych i jakie są jego obowiązki.
2. Administrator danych: Justyna Kaleta prowadząca działalność gospodarczą pod firmą Centrum Szkółkarskie „Justyna” Justyna Kaleta, ul. Trakt Św. Wojciecha 291, 80-018 Gdańsk, NIP 5831005468.

Obowiązki Administratora Danych:

1) spełnienie wskazanych w ustawie przesłanek legalizujących przetwarzanie danych osobowych;
2) obowiązek informacyjny związany z pozyskaniem danych;
3) obowiązek dochowania szczególnej staranności przy przetwarzaniu danych, w celu ochrony interesów osób, których dane dotyczą;
4) obowiązek zabezpieczenia danych;
5) obowiązek prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych;
6) obowiązek prowadzenia rejestru przetwarzania danych.

2.3 INSPEKTOR DANYCH OSOBOWYCH

1. Wyznaczenie Inspektora Ochrony Danych jest czynnością Administratora Danych. Administrator Danych nie powołał na tę funkcję, gdyż nie miał obowiązku zgodnie z przepisami RODO.
2. W następstwie powyższego określono następujące uprawnienia i obowiązki Administratora Danych, zgodne z art. 39 RODO:

   a) informowanie podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

   b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

   d) współpraca z organem nadzorczym i udział w kontrolach prowadzonych przez organ nadzoru;

   e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem;

   f) stały nadzór nad treścią Polityki Bezpieczeństwa;

   g) czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania;

h) prowadzenie jawnego rejestru zbiorów danych osobowych;

i) udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych;

j) nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych osobowych w trybie określonym w Rozdziale 3 niniejszej Polityki Bezpieczeństwa;

k) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych;

l) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych;

m) nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe;

n) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

3. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy, Polityki Bezpieczeństwa oraz załączników do niej.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia lub wykonywania usług na podstawie umowy cywilnoprawnej.

3.1 ZAKRES PRZETWARZANIA I CELE WYKORZYSTANIA DANYCH OSOBOWYCH

1. W zbiorach danych gromadzonych w systemie informatycznym zabrania się przetwarzania danych ujawniających:
    a) stan zdrowia,
    b) pochodzenie rasowe lub etniczne,
    c) poglądy polityczne,
    d) przekonania religijne lub filozoficzne,
    e) przynależność wyznaniową,
    f) przynależność partyjną lub związkową,
    g) dane genetyczne,
    h) dane biometryczne,
    i) nałogi,
    j) preferencje seksualne

    chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę.
2. Dane o skazaniach, w tym dane o niekaralności można przetwarzać jedynie zgodnie z art. 10 RODO.
3. W jednostce zabrania się używania danych wymienionych w pkt 1 do profilowania, o ile osoba, której dane dotyczą, wyraziła na to zgodę lub jest to podyktowane ważnym interesem publicznym. O profilowaniu Administrator Danych informuje osobę, której ono dotyczy, na etapie zbierania danych.
4. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie zanonimizowanej, uniemożliwiającej identyfikację osób, których dotyczą.
5. Administrator Danych lub upoważniony przez niego IOD ma obowiązek uzupełnienia, uaktualnienia, sprostowania lub usunięcia danych osobowych w przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona.

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych zawiera umowy powierzenia danych osobowych podmiotom zewnętrznym.
2. Warunkiem nieodzownym przekazania danych osobowych podmiotom zewnętrznym jest zawarcie umowy w przedmiocie powierzenia przetwarzania danych osobowych

5. ANALIZA ZAGROŻEŃ I RYZYSKA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Analiza zagrożeń i ryzyka jest głównym elementem procesu zarządzania ryzykiem bezpieczeństwa informacji. Jej celem jest wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO.
2. Ze względu na zmieniające się warunki funkcjonowania jednostki analiza ryzyka musi być wykonywana okresowo, przynajmniej raz w roku, przez IOD.
3. Analiza zidentyfikowanego zagrożenia i ryzyka polega na oszacowaniu prawdopodobieństwa jego wystąpienia i skutku jego ewentualnego wystąpienia.

6. *OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIAZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH*

1. Postanowienia dotyczące ogólnych zasad przetwarzania danych:
   1) Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych;
   2) Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności

związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych;

3) W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. czystego biurka. Zasada ta oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników;
4) Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek;
5) Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony;
6) Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem;
7) Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem;
8) Dokumenty o szczególnym znaczeniu przechowywane są w zamkniętej szafie, a dostęp do nich ma Administrator Danych;
9) Dokumenty, z których nie korzysta się na bieżąco, są archiwizowane w odrębnym archiwum, do którego dostęp zabezpieczony jest kluczem elektronicznym;
10) Osoby uprawnione do przetwarzania danych w formie elektronicznej (komputerowej) uzyskują dostęp do danych za pomocą nadanego im indywidualnego hasła przez Administratora Danych;

11) W przypadku niekorzystania z komputera przez osobę uprawnioną do przetwarzania danych przez okres 15 minut następuje blokada dostępu do danych i osoba taka może uzyskać dostęp do danych po ponownym wprowadzeniu hasła;
12) Hasła dostępu są zmieniane okresowo, ale nie rzadziej niż co trzy tygodnie.
13) Wszystkie komputery połączone są w sieć komputerową, która posiada odpowiednie zabezpieczenia antywirusowe oraz zabezpieczenia uniemożliwiające dostęp do sieci bez uprawnień (firewall);
14) Wszystkie komputery oraz serwery podlegają okresowym przeglądom antywirusowym.

7. OBOWIĄZKI INFORMACYJNE PRZY ZBIERANIU DANYCH OSOBOWYCH

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę o:

a) swojej tożsamości i podać dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie - dane kontaktowe Inspektora Ochrony Danych;

c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;

d) prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią ;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;

g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe - kryteria ustalania tego okresu;

h) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

i) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO- informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

j) informacje o prawie wniesienia skargi do organu nadzorczego;

k) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym, lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

l) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, Administrator Danych jest zobowiązany poinformować tę osobę o:

a) swojej tożsamości i podać dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie - dane kontaktowe Inspektora Ochrony Danych;

c) cele przetwarzania, do których mają posłużyć dane osobowe oraz podstawę prawną przetwarzania;

d) kategorie odnośnych danych osobowych;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;

g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe - kryteria ustalania tego okresu;

h) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO - prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;

i) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

j) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO - informacje o prawie do cofnięcia zgody w dowolnym momencie bez

wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

k) informacje o prawie wniesienia skargi do organu nadzorczego;

f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;

g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Obowiązek poinformowania wymieniony w pkt 1 niniejszego paragrafu powinien być wykonany w momencie zbierania danych z wyjątkiem sytuacji, w której Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane; przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

4. Obowiązek poinformowania wymieniony w pkt 2 niniejszego paragrafu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie z wyjątkiem sytuacji, w której:

   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.

8. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA

1. Administrator Danych zobowiązany jest do stworzenia ogólnego trybu postępowania w sytuacji naruszenia ochrony danych osobowych, który odpowiada organizacji pracy pracowników lub specjalizacji prowadzonej działalności.
2. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych:
   1) Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informacje

mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Danych;

2) Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Danych, osoba powiadamiająca powinna:
   - niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   - zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   - udokumentować wstępnie zaistniałe naruszenie,
   - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Danych lub osoby upoważnionej;
3) Po przybyciu na miejsce naruszenia ochrony danych osobowych Administrator Danych lub osoba go zastępująca:
   - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,
   - wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
4) Administrator Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport. Raport, o którym mowa powyżej, Administrator Danych niezwłocznie przekazuje zarządowi jednostki;
5) Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator Danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych;
6) W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

9. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Niniejszy rozdział reguluje system kontroli przetwarzania i stanu zabezpieczenia danych osobowych, kto jest odpowiedzialny za ich przeprowadzenie i jak często należy badać stan zabezpieczeń.
2. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w firmie Centrum Szkółkarskie „Justyna” sprawuje Administrator Danych Danych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
3. Czynności kontrolne przeprowadzane są co pół roku przed końcem maja i listopada każdego roku;
4. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności;
5. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u Administratora Danych;
6. Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w niniejszym Rozdziale stanowi Załącznik nr 10 do niniejszej Polityki.

INWENTARYZACJA

Dane szczególnych kategorii i dane karne Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie.

Dane niezidentyfikowane

Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

Profilowanie

Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji Administrator postępuje zgodnie z przyjętymi zasadami w tym zakresie.

Współadministrowanie

Administrator a identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

Administrator prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

Rejestr jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.

W Rejestrze dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, Administrator odnotowuje co najmniej:

(i) nazwę czynności,

(ii) cel przetwarzania,

(iii) opis kategorii osób,

(iv) opis kategorii danych,

(v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes,

(vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających),

(viii) informację o przekazaniu poza EU/EOG

(ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.

PODSTAWY PRZETWARZANIA

Administrator dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, uzasadniony cel), Administrator dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody – wskazując jej zakres, gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując konkretny cel, np. marketing własny, dochodzenie roszczeń.

Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

Administrator ułatwia osobom korzystanie z ich praw poprzez rożne działania, w tym: zamieszczenie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Administratorem w tym celu, ewentualnym cenniku żądań „dodatkowych” itp.

Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez

Administratora zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposob zintegrowany,
Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

OBOWIĄZKI INFORMACYJNE

Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
Administrator informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).
Administrator informuje osobę o planowanej zmianie celu przetwarzania danych.
Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
Administrator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

ŻĄDANIA OSÓB

Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z

ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

Nieprzetwarzanie.
Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

Odmowa.
Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

Dostęp do danych.
Na żądanie osoby dotyczące dostępu do jej danych Administrator informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art.15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Administrator nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.

Kopie danych.
Na żądanie Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator wprowadza i utrzymuje cennik kopii danych, zgodnie z kto rym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

Sprostowanie danych.
Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W

przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

Uzupełnienie danych.

Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator nie musi przetwarzać danych, które są Administratorowi zbędne). Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

Usunięcie danych.

Na żądanie osoby Administrator usuwa dane, gdy:

(1) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,

(2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

(3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

(4) dane były przetwarzane niezgodnie z prawem,

(5) konieczność usunięcia wynika z obowiązku prawnego,

(6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej). Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art..17. ust.3 RODO. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

Ograniczenie przetwarzania.

Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

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, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

Przenoszenie danych.

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

Sprzeciw w szczególnej sytuacji.

Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne

wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

Sprzeciw względem marketingu bezpośredniego.
Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

10. OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Dane osobowe przetwarzane są w lokalach znajdujących się w budynku umiejscowionym w miejscowości **Gdańsk, ul. Trakt Św. Wojciecha 291.**

BEZPIECZEŃSTWO

Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Firmę.
Analizy ryzyka i adekwatności środków bezpieczeństwa Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych.
W tym celu:
(1) Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
(2) Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
(3) Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o rożnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

(4) Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście, jak:

(i) pseudonimizacja,

(ii) szyfrowanie danych osobowych,

(iii) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

(iv) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Oceny skutków dla ochrony danych

Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. Administrator stosuje metodykę oceny skutków przyjętą w Firmie.

Środki bezpieczeństwa

Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa i są bliżej opisane w procedurach przyjętych przez Administratora dla tych obszarów.

11 ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POPUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. Justyna Kaleta dysponuje środkami technicznymi i organizacyjnymi, które zostały zastosowane przez Administratora Danych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych.
2. Zestawienie zastosowanych środków technicznych i organizacyjnych przedstawiono w Załączniku nr 9 do Polityki Bezpieczeństwa.

Załączniki

Załącznik nr 1 – Ustanowienie Inspektora Ochrony Danych

Załącznik nr 2 – Upoważnienie Inspektora Ochrony Danych do nadawania upoważnień

Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

Załącznik nr 4 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Załącznik nr 5 – Wzór Rejestru czynności Przetwarzania danych

Załącznik nr 7 - Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 8 – Wzór zgody na przetwarzanie danych osobowych

Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Załącznik nr 11 - Ewidencja udostępnień danych osobowych innym podmiotom

Załącznik nr 12 – Wzór oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa

Dokument sporządzono: Data: 25/05/2018 (dd/mm/rrrr) Miejsce: Gdańsk	**Pełen podpis Administratora Danych:**	**Pieczęć**