Polityka przetwarzania danych osobowych

Polskie Towarzystwo Analizy Transakcyjnej

§1. Polityka Ochrony Danych Osobowych

1. „Polityka ochrony danych osobowych" (dalej: Polityka) jest dokumentem wewnętrznym opisującym zasady przetwarzania danych osobowych w:
   - **Polskie Towarzystwo Analizy Transakcyjnej, ul. Grunwaldzka 42/2, 60-786 Poznań**
     NIP 7792366268 | REGON 301174477

   dalej zwane „Polskie Towarzystwo Analizy Transakcyjnej"

   Przepisy prawne:
   a) 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 – dalej RODO/ Rozporządzenie RODO;
   b) Ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2019 r. poz. 1781 ze zmianami), zwaną dalej "UODO";
   c) Rekomendacjami, stanowiskiem i wytycznymi Prezesa Urzędu Ochrony Danych Osobowych oraz Europejskiej Rady Ochrony Danych (dawniej Grupa Robocza art. 29)

§2. Zakres podmiotowy oraz przedmiotowy Polityki

1. Stanowi podstawowy i nadrzędny zbiór dokumentów opisujących sposób realizacji obowiązków Administratora wynikających z Rozporządzenia RODO oraz innych obowiązujących aktów prawnych.
2. Politykę stosuje się do przetwarzania danych osobowych:
   a) w sposób całkowicie lub częściowo zautomatyzowanych: w tym w systemach teleinformatycznych, poczcie elektronicznej, dyskach sieciowych, dyskach komputerów, urządzeniach typu pendrive, karta pamięci, dysk zdalny, serwerach lokalnych oraz tzw. rozwiązaniach chmurowych, urządzeniach mobilnych (m.in. telefony, tablety) oraz drukarkach w tym urządzeniach wielofunkcyjnych.
   b) w papierowych zbiorach danych, jeżeli stanowią one część zbioru danych albo mają być włączone do takiego zbioru.

§3. Podmioty odpowiedzialne

1. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator danych osobowych, przy czym niniejsza polityka obowiązuje wszystkie osoby przetwarzające dane osobowe u Administratora, niezależnie od łączącej obie strony formy współpracy w tym: umowa o pracę, umowy cywilnoprawnej, umowy o staż, wolontariat, praktyki i innych oraz niezależnie od posiadanego upoważnienia do przetwarzania danych osobowych.
2. Administrator w drodze uchwały może przekazać określony zakres swoich kompetencji opisanych w niniejszym dokumencie, wyznaczonej osobie .

§4. Skróty i definicje stosowane w Polityce Ochrony Danych Osobowych

1. Użyte skróty i definicje w niniejszej Polityce:

a)	Polityka – oznacza niniejszy dokument, o ile co innego nie wynika wyraźnie z kontekstu;
b)	Rozporządzenie RODO (RODO) – oznacza 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;
c)	Ustawa o ochronie danych osobowych – Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 ze zmianami);
d)	Dane osobowe – rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą" – podmiot danych); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora,

	takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
e)	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;
f)	Dane karne – oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i czynów zabronionych;
g)	Dane dzieci – oznaczają dane osób poniżej 16 roku życia;
h)	Osoba – oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
i)	Osoba upoważniona – osoba, której została nadane pisemne upoważnienie do przetwarzania danych osobowych u Administratora;
j)	Podmiot przetwarzający – oznacza organizację lub osobę, której Przedsiębiorstwo powierzyło przetwarzanie danych osobowych (np. firma księgowa, prawnicza, usługodawca IT);
k)	Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
l)	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;
m)	Prawa RODO – prawa osób, których dane osobowe dotyczą, przysługujące im na gruncie Rozporządzenia RODO, tj. prawo do informacji, prawo dostępu do danych, prawo do sprostowania danych, prawo do usunięcia danych – „prawo do bycia zapomnianym", prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu, prawo do cofnięcia zgody na przetwarzanie danych, prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji w tym profilowaniu, prawo do złożenia skargi do Urzędu Ochrony Danych Osobowych;
n)	Transgraniczne przetwarzania - oznacza przekazanie danych do państw trzecich lub organizacji międzynarodowych;
o)	IOD lub Inspektor - oznacza Inspektora Ochrony Danych;
p)	RCPD lub Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych;
q)	PUODO – Prezes Urzędu Ochrony Danych Osobowych – organ nadzorczy w Polsce, właściwy w sprawach ochrony danych osobowych;
r)	Administrator danych osobowych lub Administrator - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
s)	Przedsiębiorstwo – oznacza podmioty wskazane w §1 niniejszej Polityki
t)	Analiza DPIA – oznacza ocenę skutków planowanych operacji przetwarzania danych osobowych, przeprowadzana jest przez Administratora, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
u)	Privacy by design – oznacza uwzględnienie ochrony danych osobowych w fazie projektowania;

v) Privacy by default – oznacza domyślną ochronę danych osobowych, poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, zakładające ochronę prywatności;

2. Pojęcia, które nie zostały uwzględnione w Polityce, mają znaczenie zgodnie z Rozporządzeniem RODO oraz dokumentami wewnętrznymi obowiązującymi u Administratora.

§5. Zasady ogólne ochrony danych osobowych

1. Filary ochrony danych osobowych
   a) zasada legalności – Administrator danych osobowych dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
   b) zasada bezpieczeństwa – Administrator danych osobowych zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie;
   c) zasada rozliczalności – Administrator danych osobowych dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z prawem;
   d) prawa jednostki – Administrator danych osobowych umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
2. Zasady ochrony danych osobowych - Administrator danych osobowych przetwarza dane osobowe z poszanowaniem następujących zasad, w oparciu o podstawę prawną i zgodnie z prawem (art. 5 ust. 1 Rozporządzenia RODO)
   a) rzetelnie i uczciwie;
   b) w sposób przejrzysty dla osoby, której dane dotyczą;
   c) w konkretnych celach;
   d) w niezbędnym zakresie;
   e) z dbałością o prawidłowość danych;
   f) nie dłużej niż potrzeba;
   g) zapewniając odpowiednie bezpieczeństwo – integralność i poufność.
3. Zasada rozliczalności: wszelkie czynności podejmowane w celu realizacji niniejsze Polityki jak i w zakresie dotyczących przetwarzania oraz ochrony danych osobowych u Administratora danych osobowych muszą być należycie dokumentowane przez osoby, które podejmują te czynności, tak aby Administrator w każdym momencie mógł wykazać przestrzeganie RODO zgodnie z zasadą rozliczalności opisaną w art. 5 ust. 2 Rozporządzenia RODO.
4. System ochrony danych osobowych
   a) **Inwentaryzacja danych**: Administrator danych osobowych dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych, w tym: przypadków przetwarzania danych szczególnych kategorii i danych karnych, przypadków przetwarzania danych dzieci, profilowania, wespół administrowania danymi;
   b) **Rejestr**: Administrator danych osobowych prowadzi i utrzymuje Rejestr Czynności Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych;
   c) **Podstawy prawne**: Administrator danych osobowych zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze z uwzględnieniem w szczególności: art. 6, 9, 10 i 22 Rozporządzenia RODO;
   d) **Obsługa praw jednostki**: Administrator danych osobowych spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
      i. obowiązki informacyjne: Administrator danych osobowych przekazuje osobom, których dane dotyczą informacje opisane w art. 13 i 14 Rozporządzenia RODO i zapewnia dokumentowanie realizacji tych obowiązków m.in. poprzez klauzule informacyjne, politykę prywatności;
      ii. możliwość wykonywania żądań: Administrator danych osobowych weryfikuje i zapewnia możliwość efektywnego wykonywania każdego typu żądania przez siebie i swoich przetwarzających (w tym dalszych przetwarzających);
      iii. obsługa żądań: Administrator danych osobowych zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
      iv. zawiadamianie o naruszeniach: Administrator danych osobowych stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5. Bezpieczeństwo: Administrator danych osobowych zapewnia odpowiedni poziom bezpieczeństwa danych, w tym w szczególności:
   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 jest wysokie;
   c) dostosowuje środki ochrony danych do ustalonego ryzyka;
   d) posiada system zarządzania bezpieczeństwem informacji;
   e) stosuje procedury pozwalające na identyfikację, ocenę i zidentyfikowanego naruszenia ochrony danych.
6. Przetwarzający: Administrator danych osobowych posiada procedurę weryfikacji podmiotów, którym powierza przetwarzanie danych osobowych.
7. Privacy by design: Administrator danych osobowych uwzględnia ochronę danych w fazie projektowaniam.in. nowego projektu, inwestycji.

§6. Rejestr czynności przetwarzania danych

1. 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.
2. Administrator danych osobowych prowadzi Rejestr Czynności Przetwarzania Danych, w których inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi danych osobowych rozliczania większości obowiązków ochrony danych.

§7. Obsługa praw jednostki i obowiązek informacyjny

1. Administrator danych osobowych w związku z realizacją praw jednostki i spełnieniem obowiązków informacyjnych:
   a) dba o czytelność i styl przekazywania informacji i komunikacji z osobami, których dane przetwarza;
   b) ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym w szczególności poprzez zamieszczanie na stronie internetowej informacji o prawach osób, sposobie korzystania z nich, metodach kontaktu z Administrator danych osobowych w tym celu;
   c) dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób;
   d) dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób;
   e) wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

2. Administrator danych osobowych spełniając obowiązek informacyjny w szczególności:
   a) określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych;
   b) informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby art. 13 Rozporządzenia RODO;
   c) informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie nie bezpośrednio od tej osoby art. 14 Rozporządzenia RODO;
   d) określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie jest to możliwe, np. tabliczka informacyjna o objęciu obszaru monitoringiem wizyjnym;
   e) informuje osobę o planowanej zmianie celu przetwarzania danych;
   f) informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe);
   g) informuje o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą;
   h) bez zbędnej zwłoki powiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

§8. Żądania osób

1. Dostęp do danych: na żądanie osoby dotyczącej dostępu do jej danych Administrator danych osobowych informuje osobę, czy przetwarza jej dane oraz informuje o szczegółach przetwarzania zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

2. Kopie danych: na żądanie osoby, której dane dotyczą, Administrator danych osobowych wydaje kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Za kolejne kopie danych Administrator danych osobowych zastrzega prawo do pobierania opłat.
3. Sprostowanie danych: Administrator danych osobowych dokonuje sprostowania nieprawdziwych / nieprawidłowych danych na żądanie osoby, której dane dotyczą. Administrator danych osobowych ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator danych osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.
4. Uzupełnienie danych: Administrator danych osobowych uzupełnia i aktualizuje dane na żądanie osoby, której dane dotyczą. Administrator danych osobowych ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator danych osobowych może polegać na oświadczeniu osoby co do uzupełnienia danych, chyba że istnieją podstawy, aby uznać to oświadczenie za niewiarygodne.
5. Usunięcie danych: na żądanie osoby, której dane dotyczą Administrator danych osobowych usuwa dane, gdy:
   a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;
   b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
   c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
   d) dane były przetwarzane niezgodnie z prawem;
   e) konieczność usunięcia wynika z obowiązku prawnego;
   f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
6. Administrator danych osobowych 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.
7. W przypadku, gdy dane podlegające usunięciu zostały upublicznione przez Przedsiębiorcę, Przedsiębiorca podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.
8. W przypadku usunięcia danych Administrator danych osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.
9. Realizacja praw osób fizycznych w zakresie przetwarzania danych osobowych odbywa się na podstawie złożenia drogą elektroniczną, pocztową lub osobiście w siedzibie Administratora – Wniosku o realizację praw osoby, której dane dotyczą zgodnie z Rozporządzeniem RODO oraz poprzez właściwą identyfikację osoby, której dane dotyczą.

§9. Ograniczenie przetwarzania

1. Administrator danych osobowych dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
   a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawdziwość/prawidłowość;
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych,
   c) żądając w zamian ograniczenia ich wykorzystywania;
   d) Administrator danych osobowych nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane
   e) dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   f) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją do czasu
   g) stwierdzenia, czy po stronie Administrator danych osobowych zachodzą prawnie uzasadnione podstawy nadrzędne
   h) wobec podstaw sprzeciwu.
2. W trakcie ograniczenia przetwarzania Administrator danych osobowych 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.
3. W przypadku ograniczenia przetwarzania danych Administrator danych osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.

§10. Przenoszenie danych

1. Na żądanie osoby, której dane dotyczą Administrator danych osobowych 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, jeżeli przetwarzanie odbywa się:
   a) na podstawie zgody tej osoby – art. 6 ust. 1 lit a) lub art. 9 ust 2 lit.a Rozporządzenia RODO) lub,
   b) na podstawie umowy - art. 6 ust.1 lit. b) Rozporządzenia RODO,
   c) w sposób zautomatyzowany.

§11. Sprzeciw wobec przetwarzania

1. Jeżeli osoba, której dane dotyczą zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora danych osobowych w oparciu o:
   a) art. 6 ust. 1 lit f) Rozporządzenia RODO – prawnie uzasadniony interes Administratora,
   b) profilowanie na podstawie art. art. 6 ust. 1 lit f) Rozporządzenia RODO,

   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.
2. Sprzeciw względem marketingu bezpośredniego: jeżeli osoba, której dane dotyczą zgłosi sprzeciw względem przetwarzania jej danych przez Administratora danych osobowych na potrzeby marketingu bezpośredniego, Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

§12. Minimalizacja danych osobowych

1. Administrator danych osobowych dba o minimalizację przetwarzania danych pod kątem adekwatności danych do celów, dostępu do danych, czasu przechowywania danych.
2. Minimalizacja zakresu: Administrator danych osobowych zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO w Przedsiębiorstwie.
3. Administrator danych osobowych dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
4. Minimalizacja czasu:
   a) Administrator danych osobowych wdraża mechanizmy kontroli cyklu życia danych osobowych, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
   b) Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez przedsiębiorstwo. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.
5. Minimalizacja dostępu:
   a) Administrator danych osobowych stosuje ograniczenia dostępu do danych osobowych:
      i. prawne (zobowiązania do poufności, zakresy upoważnień),
      ii. fizyczne (strefy dostępu, zamykanie pomieszczeń, szaf),
      iii. logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe, hasła).
   b) Administrator danych osobowych dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
   c) Administrator danych osobowych dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

§13. Bezpieczeństwo

1. Administrator danych osobowych zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Administrator danych osobowych.

2. Analiza ryzyka i adekwatności środków bezpieczeństwa. Administrator danych osobowych przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a) Administrator danych osobowych zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych m.in. poprzez przeprowadzania szkoleń dla pracowników, współpracowników, organizowanie kampanii informacyjnych, szkolenia e-learningowe zakończone testem wiedzy.
   b) Administrator danych osobowych kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
   c) Administrator danych osobowych przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii, w tym analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
3. Administrator danych osobowych ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, środki zapewniające ciągłość działania zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
4. Ocena skutków dla ochrony danych (DPIA): Administrator dokonuje oceny skutków przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
5. 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 w przedsiębiorstwie.
6. Zgłaszanie naruszeń: Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia. Szczegółowa procedura postępowania w przypadku naruszenia opisana została w Instrukcji postepowania w sytuacji naruszenia ochrony danych osobowych.

§14. Przetwarzający

1. Administrator danych osobowych posiada zasady weryfikacji podmiotów przetwarzających dane osobowe w imieniu Administratora opracowane, w odrębnej procedurze, w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze.
2. Administrator opracował oraz przekazał do stosowania wzór Umowy powierzenia przetwarzania danych osobowych.

§15. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Zasady przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, poza Europejski Obszar Gospodarczy odbywa się zgodnie z zasadami opisanymi w Rozdziale V Rozporządzenia RODO.

§16. Projektowanie prywatności

1. Administrator danych osobowych zarządza zmianą mającą wpływ na prywatność m.in. przy realizacji projektów i inwestycji, w taki sposób, aby:
   a) umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych,
   b) zachować zasadę minimalizacji przetwarzania danych;
   c) ocenić wpływ na prywatność oraz ochronę danych.

§17. Procedura DPIA (Data Protection Impact Assessment) - Ocena skutków dla ochrony danych

1. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza administrator danych, uwzględniając co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora danych;
b) ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.

2. DPIA jest przeprowadzane w szczególności:
a) przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie,
b) jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
c) jeżeli krajowy organ nadzorczy albo Europejska Rada Ochrony Danych wskaże dany rodzaj przetwarzania w wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych.
3. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

§18. Inspektor ochrony danych

1. Administrator ma prawo wyznaczyć Inspektora ochrony danych osobowych, przy czym informację o Inspektorze danych osobowych przekaże wszystkim pracownikom, Urzędowi Ochrony Danych Osobowych oraz podmiotom zewnętrznym m.in. poprzez umieszczenie informacji w Polityce prywatności, klauzuli informacyjnej, danych kontaktowych na stronie internetowej.
2. Inspektor ochrony danych będzie wyznaczony w oparciu o przepisy Rozporządzenia RODO.

Niniejsza Polityka Ochrony Danych Osobowych wchodzi w życie z dniem 25 maja 2018 r.