Polityka Ochrony Danych Osobowych oraz Bezpieczeństwa Systemów Informacji

Niniejszy dokument został stworzony dla AGNIESZKA HAŁAS

z siedzibą w Krośnie Odrzańskim, przy ul. Prądzyńskiego 11

zarejestrowaną pod numerem NIP: 9261685148. (zwaną dalej: **Administratorem**).

Spis treści

1. Terminologia

1.1. Wstęp

Niniejszy dokument, zatytułowany „Polityka ochrony danych osobowych oraz Bezpieczeństwa Systemów Informacji" (dalej: „**Polityka**") stanowi mapę wymogów, zasad i regulacji ochrony danych osobowych jak też bezpieczeństwa informacji w systemach używanych przez Administratora. Polityka stanowi opis zabezpieczania systemów informacji Administratora, jak również politykę ochrony danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej: „**RODO**").

1.2. Podstawy stworzenia dokumentu

Administrator, wypełniający we wskazany w niniejszym dokumencie sposób swoje obowiązki nałożone na niego przez RODO jak również przepisy wprowadzające RODO do polskiego porządku prawnego, to w rozumieniu wyżej wskazanych aktów prawnych również:

- współpracownicy Administratora,
- procesy biznesowe i metody pracy Administratora,
- wiedza o Klientach Administratora,
- partnerzy biznesowi Administratora i jego relacje z nimi.

Zaufanie pomiędzy Klientami a naszą firmą i współpracownikami oraz nasze dziedzictwo to elementy, które sprawiają, że wartość Administratora wyróżnia nas i tworzy naszą tożsamość, odzwierciedla naszą kulturę. Naszym obowiązkiem jest ich ochrona.

1.3. Systemy Informacyjne jako wyznacznik poziomu bezpieczeństwa biznesu

Systemy informatyczne rozwijają się coraz bardziej każdego dnia, ułatwiają wymianę informacji. Z tych powodów Systemy Informatyczne Administratora stały się głównym narzędziem w:

- rozwoju i dzieleniu się naszym dziedzictwem, co pozwala nam być bardziej dynamicznymi i skutecznymi;

- tworzeniu i utrzymaniu z naszymi Klientami i pracownikami relacji trwałych i godnych zaufania, umożliwia to zapewnienie wysokiej wydajności oraz zapewnienie usług dostosowanych do potrzeb i zwyczajów każdego człowieka.

Nasz system IT jest kluczowym czynnikiem w rozwoju naszego dziedzictwa i rozwoju pełnego zaufania Klientów.

Jednak jesteśmy świadomi, że w dzisiejszych czasach nasze systemy IT podlegają wszelkiego rodzaju zagrożeniom, które w razie wystąpienia incydentu mogą mieć negatywne konsekwencje dla naszej działalności, w związku z czym dochowujemy należytej staranności by chronić je w odpowiedni sposób i codziennie stawiać czoła nowym wyzwaniom w tym zakresie jak również dążyć do nieustannego zwiększania bezpieczeństwa używanych przez nas systemów informatycznych.

1.4. Zagrożenia w zakresie bezpieczeństwa IT

Poziom ryzyka związanego z bezpieczeństwem IT jest ustalany na podstawie globalnej strategicznej mapy ryzyka. Głównymi zagrożeniami bezpieczeństwa IT są:

- niezdolność Systemu Informacji w momencie krytycznym dla biznesu;
- niezdolność do wykrywania nadużyć wewnętrznych w systemach informatycznych;
- błędy decyzyjne z powodu błędnych danych finansowych;
- utrata danych lub ujawnienie zapisów danych Klienta;
- utrata przewagi konkurencyjnej w wyniku wycieku danych;

Nasze dziedzictwo i systemy informacji, które wspierają nasze krytyczne procesy biznesowe są uwzględnione w zagrożeniach bezpieczeństwa.

1.5. Główne cele bezpieczeństwa systemów IT

Tak, aby uniknąć ryzyka, musimy chronić nasze wrażliwe systemy informacyjne w praktyce. Strategia ta jest zawarta w Polityce Bezpieczeństwa Systemów Informacji i odnosi się do głównych celów bezpieczeństwa, które mają na celu zmniejszenie ryzyka na akceptowalnym poziomie.
Główne cele bezpieczeństwa są opisane szczegółowo w rozdziale 4 niniejszego dokumentu.

Polityka Ochrony Danych Osobowych i Bezpieczeństwa Systemów Informacji jest podstawowym dokumentem bezpieczeństwa korporacyjnego Administratora, dostosowanym do strategicznych zagrożeń i dokumentem spójnym z RODO.

2. Prezentacja polityki bezpieczeństwa

2.1. Cel

Polityka Ochrony Danych Osobowych i Bezpieczeństwa Systemów Informacji Administratora ma na celu inspirowanie, zachęcanie i zwiększanie zaufania wśród użytkowników (współpracowników, Klientów, partnerów) w systemach informacji i świadczonych usługach.

2.2. Zasady bezpieczeństwa przy podejściu globalnym

Mając na myśli globalne bezpieczeństwo systemów informacyjnych Administratora, wyróżniamy następujące zasady motywowania:

- realizm: polityka bezpieczeństwa IT zbudowana jest krok po kroku, dostosowana do poziomu wielkości Administratora, dążąc przy tym do stopniowej poprawy (podejście dynamiczne),

- pragmatyzm: rozwiązania (zasady, środki, procedury) są stosowane w taki sposób, aby znaleźć odpowiedni kompromis pomiędzy efektywnością, prostotą i kontrolą kosztów, koncentrując się na obsłudze klienta,

- odpowiedzialność: organizacja systemu zarządzania bezpieczeństwem jest dostosowana do Administratora, autonomiczna i odpowiedzialna, działająca w synergii wspólnego interesu,

- spójność: działania osób współpracujących z Administratorem są zgodne z bezpieczeństwem, obowiązującym na terenie działalności Administratora z uwzględnieniem poprawy współpracy i wspólnej wizji (globalne podejście),

- przewidywanie: większe bezpieczeństwo przewidywania (w projektach IT, definicjach usług, tworzeniu nowych projektów lub ich ewolucji), bardziej określone działania i aplikacje mogą być dostosowane skutecznie i trwale,

2.3. Projektowanie bezpieczeństwa danych przez Administratora

Architektura bezpieczeństwa Administratora jest oparta na wzorcowym dokumencie odniesienia. Wzorzec ten składa się z:

- niniejszego dokumentu, który określa strategiczne punkty powiązane z bezpieczeństwem u Administratora i przełożenie ich na fundamentalne cele: stanowi podstawy we wszystkich kwestiach bezpieczeństwa Administratora;

- standardów bezpieczeństwa definiujących stopnie bezpieczeństwa, które będą osiągane przez realizację podstawowych celów bezpieczeństwa określonych przez Administratora i to na różne sposoby, w tym przy użyciu narzędzi i najlepszych praktyk znanych Administratorowi;

- procedur i trybów operacyjnych opisujących technicznie sposoby wdrożenia środków bezpieczeństwa.

Ta architektura bezpieczeństwa jest wdrożona u Administratora i przyjmuje ona formę Polityki Ochrony Danych Osobowych i Bezpieczeństwa Systemów Informacji tak, aby umożliwić realizację konkretnych celów.

2.4. Schemat zastosowania

Niniejszy dokument odnosi się do wszystkich systemów informacyjnych, używanych przez Administratora, w tym w szczególności do:

- wszystkich współpracowników Administratora;
- wszystkich partnerów (przedsiębiorcy, w tym spółki handlowe, usługodawcy, podwykonawcy);
- wszystkich procesów i aplikacji;
- wszystkich komponentów systemów informatycznych (komputery biurowe, laptopy, smartfony, tablety, itp).

2.5. Przegląd polityki bezpieczeństwa systemów informacji

W celu zapewnienia jej stałej przydatności, adekwatności i skuteczności, Polityka Ochrony Danych Osobowych i Bezpieczeństwa Systemów Informacji Administratora jest **uaktualniana co dwa lata**, lub w przypadku istotnych zmian przy procesie ponownej oceny jej zasadności i w procesie określenia ryzyk strategicznych.

3. Podstawowe cele BEZPIECZEŃSTWA

3.1. Kultura bezpieczeństwa

Osoby współpracujące z Administratorem są głównymi elementami w systemach bezpieczeństwa informacji. To oni stanowią trzon w strategii bezpieczeństwa. Jednak ich działania mogą również prowadzić do poważnych wypadków z powodu nieznajomości ryzyka i nieprzestrzegania najlepszych praktyk.

W konsekwencji tego, powinien być realizowany program informacyjny i szkoleniowy tak, aby szerzyć kulturę bezpieczeństwa u wszystkich pracowników Administratora z uwzględnieniem osób trzecich (partnerów, podwykonawców, itd.) przez cały okres spędzony u Administratora i na wyjeździe.

3.2. Regulacje prawne dotyczące danych Klienta

Systemy informatyczne są przedmiotem licznych regulacji prawnych (o ochronie danych osobowych, ochrony informacji finansowej) lub przepisów o ochronie informacji (płatność kartą kredytową).

Regulacje prawne nie są opcją, lecz obowiązkiem. W związku z tym, monitorowanie regulacyjne odnoszące się do bezpieczeństwa IT musi być zgodne z lokalnymi przepisami prawnymi. Doradztwa w zakresie wymogów prawnych należy szukać u radców prawnych.

Co więcej, w systemach informacji muszą być stosowane wszystkie niezbędne środki bezpieczeństwa uwzględniające wymogi regulacyjne.

3.3. Kontrola dostępu i zezwolenia

System Informacji przechowuje większość danych, co więcej, niektóre informacje są w większym stopniu niż inne narażone na wyciek ze względu na swoją treść, ale również ze względu na nieustannie zmieniające się zagrożenia informatyczne. Niektóre spośród tych danych podlegają regulacji lub zobowiązaniom prawnym (dane Klienta itd.). Dostęp do informacji poufnych musi być w naturalny sposób ściśle ograniczony.

W związku z tym, procedury oraz działania operacyjne są wprowadzone w celu kontrolowania dostępu do systemu Informacji, tam, gdzie jest to konieczne. Są to następujące zasady:

- jednoznaczna identyfikacja użytkowników,

- bezpieczne uwierzytelnianie użytkowników, co oznacza, że środki do autentyfikacji są osobiste i poziom bezpieczeństwa jest zapewniony,

- niższe przywileje, co oznacza, że użytkownicy posiadają uprawnienia dostosowane do ich stanowiska, nie mniej i nie więcej,

- potrzeba wiedzy - to oznacza, że użytkownicy mają dostęp tylko do tych usług niezbędnych do wykonywania swojej pracy, nie więcej i nie mniej.

3.4. Umożliwienie śledzenia operacji

Liczne wrażliwe operacje przechodzą przez system informacyjny. Warto wymienić tutaj operacje finansowe, operacje na Kliencie lub zarządzanie pracownikami. Operacje te mają być monitorowane zgodnie z zaadaptowanym procesem przepływności.

W konsekwencji, możliwość śledzenia operacji wrażliwych jest zapewniana przez:

- definicję polityki zapisu logów dostosowanym do wagi operacji monitorowania i zgodności z obowiązującymi wymogami prawnymi,

- definiowanie i wdrażanie automatycznych rozwiązań do bezpiecznego zarządzania wszystkimi aspektami procesu zarządzania dziennikami (generowanie, gromadzenie, przechowywania, archiwizacji, czas przechowywania),

4. Polityka Ochrony danych osobowych

Polityka w swojej treści przedstawia:

a) opis zasad ochrony danych obowiązujących u Administratora,
b) jeśli jest to niezbędne – również odwołania do załączników uszczegółowiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest zarząd Administratora, a w ramach zarządu:

a) członek zarządu lub członkowie zarządu, którym powierzono nadzór nad obszarem ochrony danych osobowych,
b) osoba wyznaczona przez zarząd do zapewnienia zgodności z ochroną danych osobowych.

Za stosowanie niniejszej Polityki odpowiedzialni są:

a) Administrator,
b) wszyscy członkowie personelu Administratora.

Administrator powinien też zapewnić zgodność postępowania kontrahentów z niniejszą Polityką w odpowiednim zakresie, szczególnie w przypadkach gdy mamy do czynienia z przekazaniem im danych osobowych przez Administratora. W tym celu Administrator zawiera z kontrahentami, którzy uzyskują dostęp do danych osobowych klientów Administratora umowy o powierzenie przetwarzania danych osobowych.

4.1. Ochrona danych osobowych u Administratora – procedury ochrony.

4.1.1. Podstawy ochrony danych osobowych:

1. **Legalność** – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem i jedynie na podstawie obowiązujących przepisów prawa.
2. **Bezpieczeństwo** – Administrator zapewnia poziom bezpieczeństwa danych odpowiadający sektorowi jego działalności, podejmując stale działania w tym zakresie (Administrator korzysta w tym zakresie z usług oferowanych przez podmioty zawodowo trudniące się problematyką ochrony danych, takich jak kancelarie prawne).
3. **Prawa osób fizycznych** – Administrator umożliwia osobom fizycznym, których dane przetwarza, wykonywanie swoich praw przyznanych przez przepisy RODO i realizuje te prawa, stosując się do wszystkich, opisanych w niniejszej Polityce stadiów ochrony danych.
4. **Rozliczalność** – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność. Dokumentacja przechowywana jest w miejscach odpowiednio chronionych, przy zachowaniu zasad bezpieczeństwa przed wyciekiem danych.

4.1.2. Zasady ochrony danych

Administrator przetwarza dane osobowe mając na uwadze przede wszystkim, by przetwarzanie danych następowało:

1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm),
2. rzetelnie i z poszanowaniem praw jednostki (rzetelność),
3. w sposób przejrzysty dla osoby, której dane dotyczą, mając na uwadze, że osoby fizyczne mają ograniczony czas na zaznajomienie się ze sposobami przetwarzania danych, stosowanymi przez Administratora (transparentność),
4. w konkretnych celach i nie w celu bliżej niesprecyzowanych celów – przetwarzanie danych „na przyszłość" (minimalizacja),
5. jedynie w takim zakresie, jaki jest niezbędny (adekwatność),
6. z dbałością o to, by przetwarzane przez Administratora dane były zgodne z rzeczywistością (prawidłowość),
7. nie dłużej niż jest to niezbędne do wykonania obowiązków wynikających ze stosunku prawnego lub faktycznego łączącego Administratora z drugą stroną i jedynie w takim zakresie, w jakim Administrator powiadomił osobę fizyczną o czasie, w jakim dane będą przetwarzane (czasowość),
8. zapewniając odpowiednie bezpieczeństwo danych z uwagi na potencjalne ryzyka i zagrożenia związane z operacjami, dokonywanymi na danych osobowych (bezpieczeństwo).

4.1.3. Stosowane systemy ochrony danych

System ochrony danych osobowych u Administratora składa się przede wszystkim takich składników, jak:

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 osób niezidentyfikowanych przez Administratora (dane niezidentyfikowane),
    b. przypadków przetwarzania danych dzieci,
    c. profilowania,
2. **Rejestr Przetwarzania Danych Osobowych**. Administrator opracowuje, prowadzi i utrzymuje rejestr czynności dokonywanych na danych osobowych u Administratora (dalej: „**Rejestr**" lub „**RCPD**"). Rejestr jest narzędziem rozliczania zgodności przetwarzania danych osobowych u Administratora z powszechnie obowiązującymi przepisami prawa.
3. **Podstawy prawne**. Administrator zapewnia, identyfikuje oraz weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
    a. utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość, by w prosty sposób zdeterminować możliwość komunikacji z osobami fizycznymi w określonych celach;
    b. uzasadnia przypadki, gdy Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora.
4. **Obsługa praw jednostki**. Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw (art. 12 ust. 3 RODO), realizując otrzymane w tym zakresie żądania, w tym:
    a. **obowiązek informacyjny**. Administrator przekazuje osobom wymagane informacje przy zbieraniu danych i w innych sytuacjach (na początkowym etapie wdrażania przepisów RODO, Administrator legalizuje istniejącą bazę danych w zakresie w jakim chodzi o powiadomienie o nowych uprawnieniach przyznanych osobom fizycznym przez RODO) oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków, tak by móc

wykazać ich wypełnienie w przypadku ewentualnej kontroli Urzędu Ochrony Danych Osobowych,

b. **Wykonanie żądań osób fizycznych**. Administrator zapewnia możliwość wykonania żądań kierowanych do niej przez osoby fizyczne, których dane osobowe przetwarza zarówno przez siebie i swoich przetwarzających (obowiązki procesorów nałożone w drodze umów o powierzenie przetwarzania danych osobowych),
c. **obsługa żądań osób fizycznych**. Administrator zapewnia odpowiednie nakłady finansowe i personelowi, jak również procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO, jak również by ich wykonanie zostało każdorazowo udokumentowane we właściwy sposób,
d. **zawiadamianie o naruszeniach**. Administrator stosuje procedury, które pozwalają ustalić konieczność zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych. W tym celu członek zarządu w osobie do tego wyznaczonej, nadzoruje procesy przetwarzania danych w ten sposób, by zawiadomienie o naruszeniach mogło nastąpić niezwłocznie, jednak zawsze w terminach nie późniejszych niż określone w powszechnie obowiązujących przepisach prawa.

5. **Minimalizacja**. Administrator wdrożył zasady i metody kompatybilne z określoną przepisami RODO zasadą minimalizacji, w ten sposób by nie przetwarzać danych osobowych zbędnych i nadmiarowych. Administrator poprzez zasadę minimalizacji dąży, by w jego bazie danych nie znajdowały się dane, które nie są absolutnie niezbędne do poprawnego wykonywania stosunków prawnych i faktycznych łączących Administratora z jej klientami i kontrahentami (*privacy by default*), a w tym:
    a. zasady pomagające efektywnie zarządzać adekwatnością danych już na etapie zbierania danych (formularze przystosowane do niepobierania danych nadmiarowych),
    b. zasady zarządzania dostępem do danych osób fizycznych, które o taki dostęp wnioskują, poprzez odpowiednie przeszkolenie osób odpowiedzialnych za te kwestie na terenie działalności Administratora jak również przygotowanie odpowiedniej procedury działania,
    c. zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności, a w efekcie niezwłocznego usuwania danych osobowych osób fizycznych, gdy wygaśnie podstawa prawna do takiego działania.

6. **Bezpieczeństwo**. Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
    a. przeprowadza niezbędne analizy ryzyka dla czynności przetwarzania danych lub ich kategorii, stosując przy tym odpowiednią skalę ryzyk, stanowiącą załącznik do Rejestru Czynności Przetwarzania Danych,
    b. przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie ze względu na ich charakter lub miejsce przechowywania,
    c. dostosowuje środki ochrony danych do ustalonego ryzyka,
    d. posiada wewnętrzne procedury zarządzania bezpieczeństwem informacji,
    e. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

7. **Podmioty Przetwarzające**. Administrator posiada zasady weryfikacji podmiotów przetwarzających dane na rzecz Administratora, wymogów co do warunków przetwarzania (w tym celu z każdym podmiotem przetwarzającym dane osobowe powierzone przez Administratora zawierana jest umowa o powierzenie przetwarzania danych osobowych), zasad weryfikacji wykonywania umów powierzenia, przede wszystkim poprzez stosowanie wymogów

przedstawienia przez podmioty przetwarzające stosowanych przez Administratora procedur zabezpieczenia, będących załącznikami do umów powierzenia przetwarzania danych w imieniu Administratora.

8. **Przekazywanie danych do państw trzecich**. Administrator weryfikuje czy dane osobowe osób fizycznych nie są przekazywane do państw trzecich (tj. poza teren Unii Europejskiej, Norwegii, Lichtensteinu i Islandii) lub do organizacji międzynarodowych oraz zapewnia zgodne z prawem warunki takiego przekazywania, jeśli ma ono miejsce.

9. **Privacy by design**. Administrator zarządza zmianami wpływającymi na prywatność i kontroluje je w odpowiedni ze względu na przepisy o ochronie danych osobowych sposób. W tym celu procedury uruchamiania nowych projektów i inwestycji przez Administratora 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 każdorazowo weryfikuje czy nie zachodzi przypadek transgranicznego przetwarzania danych osobowych, by w tym celu wypełnić wszystkie prawne obowiązki nakładane w związku z tym na administratora.

4.2. INWENTARYZACJA

4.2.1. Dane szczególnych kategorii i dane karne

Administrator nie identyfikuje przypadków, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne w związku z czym nie jest niezbędne utrzymywanie mechanizmów dedykowanych zapewnieniu zgodności przetwarzania tych kategorii danych osobowych z prawem.

4.2.2. Dane niezidentyfikowane

Administrator rozpoznaje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, w związku z czym gdy zachodzi taka konieczność, podejmuje wszystkie niezbędne czynności ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

4.2.3. Profilowanie

Administrator identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych w związku z czym podejmuje wszelkie środki i starania, by ten proces odbywał się zgodnie z prawem i poszanowaniem praw osób fizycznych, których dane są przetwarzane.

4.2.4. Współadministrowanie

Administrator nie identyfikuje przypadków współadministrowania danymi osobowymi.

4.3. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH (DALEJ: „**RCPD**”)

1. RCPD Stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z podstawowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności tak, by nie tylko podmioty kontrolujące przetwarzanie danych mogły w czytelny sposób określić sposób wykonywania obowiązków nałożonych na administratora danych, ale również administrator mógł zidentyfikować wewnętrzne naruszenia i reagować na nie.
2. Administrator prowadzi RCPD, w którym inwentaryzuje i nadzoruje sposoby, w jakie wykorzystuje dane osobowe.
3. RCPD jest, obok niniejszego dokumentu, który Administrator przekazuje współpracownikom w celach edukacyjnych i informacyjnych, jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie większości obowiązków ochrony danych.
4. W RCPD dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb RCPD, Administrator odnotowuje co najmniej:

    a. nazwę czynności,
    b. jednostkę organizacyjną
    c. cel przetwarzania,
    d. kategorie osób,
    e. kategorie danych,
    f. podstawę prawną przetwarzania,
    g. źródło danych,
    h. planowany termin usunięcia kategorii danych,
    i. nazwę współadministratora i jego dane kontaktowe (jeśli dotyczy),
    j. nazwę podmiotu przetwarzającego i jego dane kontaktowe (jeśli dotyczy)
    k. kategorie odbiorców (jeśli dotyczy),
    l. nazwę systemu lub oprogramowania, używanego przy przetwarzaniu danych osobowych,
    m. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 RODO,
    n. Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu),
    o. Jeśli transfer i art. 49 ust. 1 akapit drugi RODO - dokumentacja odpowiednich zabezpieczeń.

5. Wzór RCPD stanowi Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych”, Wzór RCPD zawiera także kolumny niewymagane prawem. W kolumnach nieobowiązkowych Administrator rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść RCPD ułatwia zarządzanie zgodnością ochrony danych i rozliczenia z niej. Do rejestru Administrator dołącza skalę ryzyk, która w pełniejszy sposób pozwala określić zagrożenia związane z przetwarzaniem konkretnych kategorii danych, by w najlepszy możliwy sposób dopasować środki ochrony do kategorii przetwarzanych danych.

4.4. PODSTAWY PRAWNE PRZETWARZANIA

1. Administrator dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania, by móc dostosowywać rejestr do nowelizacji aktów prawnych, z których wynikają obowiązki.

2. Poprzez wskazanie w dokumentach ogólnej podstawy prawnej (zgoda, umowa, obowiązek prawny, żywotne interesy, uzasadniony cel Administratora), Administrator dookreśla podstawę w precyzyjny sposób, gdy jest to potrzebne i niezbędne ze względu na kategorię danych i zasadę przejrzystości. W ten sposób Administrator wskazuje np. zakres uzyskiwanej zgody, przedstawiając jednocześnie cel, w jakim jest ona uzyskiwana, a gdy podstawą jest prawo – wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne itp. – wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując konkretny cel, np. marketing bezpośredni, obronę przed roszczeniami jak również możliwość ich dochodzenia.

3. Administrator wdraża metody zarządzania zgodami, umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu na każdym etapie przetwarzania danych, zgody na komunikację na odległość zgodnie z przepisami ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2004 Nr 171 poz. 1800) oraz ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 Nr 144 poz. 1204) jak również rejestracją odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, żądanie usunięcia danych itp.).

4.5. PROCEDURY OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

1. Administrator dba o czytelność przekazywanych informacji i komunikacji z osobami, których dane przetwarza, tak by mieć pewność, że osoba zapoznała się z przekazywanymi informacjami oraz że w pełni zrozumiała ich treść. W tym celu Administrator współpracuje z podmiotami zewnętrznymi (radcy prawni) w celu stworzenia obowiązków informacyjnych o treści możliwie najbardziej przejrzystej i zgodnej z przepisami powszechnie obowiązującego prawa.

2. Administrator ułatwia osobom korzystanie z ich praw poprzez działania takie jak: umieszczanie na stronie internetowej Administratora linków do informacji o prawach osób, sposobie korzystania z nich na terenie działalności Administratora, jak również metodach kontaktu z Administratorem w tym celu.

3. Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób fizycznych, których dane osobowe przetwarza poprzez stosowanie odpowiednich procedur i formularzy, za pomocą których udziela odpowiedzi na żądania i pytania kierowane do Administratora w przedmiocie ochrony danych osobowych osób fizycznych, których dane są przetwarzane.

4. Administrator wprowadza adekwatne metody identyfikacji osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych w ten sposób, by osoby nieuprawnione nie uzyskały dostępu do danych osobowych, które ich nie dotyczą.

5. W celu realizacji praw jednostki, Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób, przetwarzane przez Administratora, w celu skutecznej odpowiedzi na żądania osób fizycznych, udostępniając im dane osobowe ich dotyczące jak

również dając im możliwość skorzystania z takich uprawnień jak sprostowanie danych, ich usunięcie czy przeniesienie (w takim zakresie, w jakim to możliwe).

6. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób fizycznych w celu zachowania transparentności działania Administratora w dziedzinie ochrony danych osobowych.

4.6. OBOWIĄZKI INFORMACYJNE

1. Administrator, w porozumieniu z podmiotami zewnętrznymi (radcy prawni) określa zgodne z prawem i skuteczne sposoby wykonywania obowiązków informacyjnych.

2. Administrator informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby (art. 12 ust. 3 RODO) w przypadku, gdy rozpatrzenie jej żądania przed upływem tego terminu jest niemożliwe.

3. Administrator informuje osobę o przetwarzaniu jej danych, w sytuacji gdy dane osobowe pozyskane są bezpośrednio od tej osoby.

4. Administrator informuje osobę o przetwarzaniu danych osobowych, również w sytuacji gdy dane osobowe pozyskane są niebezpośrednio od tej osoby.

5. Administrator określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, jeśli tylko jest to możliwe (np. informacja przy wejściu do budynku o objęciu obszaru monitoringiem wizyjnym).

6. Administrator informuje osobę o planowanej zmianie celu przetwarzania danych, jeśli zachodzi taka sytuacja.

7. Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych (chyba, że wymagałoby to niewspółmiernie dużego wysiłku lub byłoby niemożliwe).

8. Administrator informuje osobę o prawie sprzeciwu jak również wszystkich przysługujących jej prawach, których źródłem jest art. 13 lub 14 RODO, względem przetwarzania jej danych osobowych najpóźniej przy pierwszym kontakcie z tą osobą.

9. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

4.7. ŻĄDANIA OSÓB FIZYCZNYCH, KTÓRYCH DANE PRZETWARZA ADMINISTRATOR

1. **Prawa osób trzecich**. Realizując prawa osób, których dane dotyczą, Administrator wprowadza gwarancje ochrony praw osób trzecich w przedmiocie ochrony ich danych osobowych. W sytuacji gdy np. wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych mogłoby wpłynąć niekorzystnie na prawa i wolności innych osób lub w sposób istotny naruszyć ich interesy prawne (np. prawa związane z ochroną danych innych osób gdy Administrator musiałby udostępnić dokumenty zawierające dane osobowe zainteresowanego, które zawierają również dane osobowe innych osób, które nie mogą być z różnych względów zanonimizowane, prawa własności intelektualnej, tajemnicę handlową lub dobra osobiste), Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub odmówić zadośćuczynienia żądaniu.

2. **Odmowa zadośćuczynienia żądaniu**. Administrator, w drodze przesłania odpowiedniego formularza, informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych w przypadku gdy z różnych względów, o których mowa w niniejszym dokumencie lub wynikających bezpośrednio z powszechnie obowiązujących przepisów prawa (np. obowiązki podatkowe) spełnienie żądania osoby jest niemożliwe.

3. **Dostęp do danych osobowych**. 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 przetwarzania odpowiada obowiązkowi informacyjnemu przy zbieraniu danych). Administrator umożliwia dostęp do danych osobowych osobie, która o to wnioskuje, jednak tylko w przypadku gdy nie zagraża to naruszeniem danych osobowych innych osób (brak możliwości zanonimizowania danych osobowych niedotyczących bezpośrednio osoby kierującej żądanie lub ryzyko udostępnienia tajemnicy handlowej itp.). Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że każda kolejna (po pierwszej) kopia danych osobowych jest kopią, za którą Administrator może pobrać odpowiednie opłaty, uzasadnione nakładem pracy związanym z jej uzyskaniem i wydaniem osobie zainteresowanej.

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

5. **Sprostowanie danych**. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby fizycznej, której dane osobowe przetwarzane przez Administratora dotyczą. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowość danych, których sprostowania się domaga.

6. **Uzupełnienie danych**. Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych w związku z faktem przekazanych już osobie fizycznej dokumentów informującym ją o celach przetwarzania (np. Administrator nie powinien zgodnie z niniejszym dokumentem przetwarzać danych, które są zbędne lub nadmiarowe). 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 okoliczności faktyczne uzasadniające obawy, że oświadczenie osoby, która kieruje żądanie jest niewiarygodne.

7. **Kopie danych**. Na żądanie, Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych, z zastrzeżeniem sytuacji zawartych w niniejszym dokumencie, związanych z możliwością naruszenia danych osobowych osób trzecich.

8. **Przenoszenie danych**. Na żądanie osoby, Administrator wydaje w powszechnie używanym formacie nadającym się do odczytu komputerowego 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.

9. **Prawo do odwołania przy przetwarzaniu danych osobowych**. Jeżeli Administrator przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, Administrator zapewnia jednocześnie możliwość odwołania się do decyzji współpracownika lub członka zarządu, upoważnionego do tego typu działania po stronie Administratora, chyba że taka automatyczna decyzja

    a. jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem,
    b. jest wprost dozwolona przepisami prawa,
    c. opiera się na wyraźnej zgodzie odwołującej osoby.

10. **Usunięcie danych**. Na żądanie osoby, Administrator usuwa dane, gdy:

    a. dane nie są niezbędne do celów, w których zostały zebranie, ani przetwarzane w innych zgodnych z prawem celach lub celach wymaganych przepisami prawa,
    b. zgoda na ich przetwarzanie została cofnięta, a Administrator nie dysponuje inną podstawą prawną przetwarzania,
    c. osoba fizyczna, której dane osobowe są przetwarzane 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 oferowanych bezpośrednio dziecku.

Administrator określa sposób realizacji prawa do usunięcia danych mając przy tym na uwadze obowiązek zapewnienia efektywnej realizacji tego prawa. Mowa przede wszystkim o zasadzie bezpieczeństwa, a także poszanowaniu obowiązku weryfikacji, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora na stronie internetowej lub w celu marketingowym wydarzenia organizowanego przez Administratora lub takiego, w którym Administrator bierze czynny udział, przy jednoczesnym założeniu otrzymania niezbędnych zgód osób, których dane osobowe są przetwarzane w ten sposób, 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.

11. **Ograniczenie przetwarzania**. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a. dane osobowe przetwarzane przez Administratora są kwestionowane przez osobę fizyczną, której dane dotyczą – na okres niezbędny z punktu widzenia weryfikacji ich prawidłowości,
b. przetwarzanie jest niezgodne z prawem, jednak osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, chcąc jedynie by ich przetwarzanie zostało ograniczone ze względu na wskazane przez nią cele,
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 jej danych osobowych – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy prawne nadrzędne wobec podstaw sprzeciwu (np. przepisy podatkowe i inne).

W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie wykorzystuje ich oraz nie przekazuje osobom trzecim, ani innym podmiotom odrębnym od Administratora i jego pracowników, uprawnionych do dostępu do przedmiotowych danych. Wyjątkiem jest wyraźna zgoda osoby, której dane dotyczą jak również ustalenie, dochodzenie lub obrona roszczeń.

W przypadku ograniczenia przetwarzania danych, Administrator na żądanie osoby, której przetwarzane dane osobowe dotyczą, informuje tę osobę o odbiorcach danych.

12. **Sprzeciw przeciwko przetwarzaniu danych osobowych**. Jeżeli osoba zgłosi umotywowany 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. Wyjątkiem od tego jest sytuacja, gdy po stronie Administratora zachodzą ważne, prawnie uzasadnione podstawy do przetwarzania, które ze względu na całokształt okoliczności i powszechnie obowiązujące przepisy prawa należy uznać za nadrzędne wobec interesów i praw osoby zgłaszającej sprzeciw.

13. **Sprzeciw względem marketingu bezpośredniego**. Jeżeli osoba fizyczna, której dane osobowe są przetwarzane przez Administratora zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego, Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania, bez wyjątków motywowanych sytuacją faktyczną lub przepisami prawa.

4.8. MINIMALIZACJA PRZETWARZANIA DANYCH

Administrator dba o minimalizację przetwarzania danych z punktu widzenia zasad, takich jak:

1. adekwatności przetwarzanych danych osobowych do celów, dla których są one przetwarzane,
2. dostępu do danych osobowych przetwarzanych przez Administratora,
3. czasu przechowywania danych osobowych.

4.8.1. Minimalizacja dostępu do danych osobowych

Administrator stosuje ograniczenia dostępu do danych osobowych, które mają charakter prawny (zobowiązania współpracowników do poufności, upoważnienia współpracowników posiadających dostęp do danych osobowych), fizyczny (dostęp do plików z danymi osobowymi tylko dla osób upoważnionych w sposób by możliwie zminimalizować ryzyko wycieku danych, zamykanie pomieszczeń) i logistyczny (przydzielenie odpowiednich haseł dostępu do danych osobowych w ten sposób, by zminimalizować ryzyko dostępu do danych osób nieupoważnionych).

Administrator stosuje również kontrolę dostępu fizycznego poprzez niedopuszczanie do miejsc pracy klientów i osób, które nie podpisały z Administratorem umowy współpracy i odpowiednich aneksów upoważniających ich do dostępu do danych jak również oświadczeń w zakresie zachowania poufności.

Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.

Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

4.8.2. Minimalizacja czasu przetwarzania danych

Administrator wdraża mechanizmy kontroli przetwarzania danych osobowych na wszystkich etapach przetwarzania, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w RCPD jak również w obowiązkach informacyjnych, przekazywanych osobom, których dane osobowe są przetwarzane.

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów informatycznych Administratora jak też z miejsc przechowywania dokumentów, zawierających dane osobowe.
Dane, o których mowa powyżej mogą być archiwizowane w uzasadnionych przypadkach oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Administratora.

4.8.3. Minimalizacja zakresu przetwarzania danych

Przy wdrażaniu do funkcjonowania Administratora RODO, Administrator zweryfikował zakres pozyskiwanych danych, zakres w jakim przedmiotowe dane są przetwarzane jak również ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania.

Administrator zobowiązuje się dokonywać okresowego przeglądu treści przetwarzanych danych osobowych, ich ilości i zakresu ich przetwarzania nie rzadziej niż raz na rok.

Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych osobowych, w sposób o którym mowa powyżej, w ramach procedur zarządzania przedmiotową zmianą (*privacy by design*).

4.9. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH PRZEZ ADMINISTRATORA

Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw osób fizycznych w związku z charakterem danych osobowych, które są przetwarzane jak również miejsc, w których dane są przechowywane.

4.9.1. Analizy ryzyka

Administrator przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

1. Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji i cyberbezpieczeństwie – wewnętrznie oraz ze wsparciem podmiotów wyspecjalizowanych (kancelarie prawne wyspecjalizowane w zakresie ochrony danych osobowych na terenie przedsiębiorstw).
2. Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają tworząc przy tym odpowiedni rejestr przetwarzania danych, na którym opiera się Administrator przy doborze procedur ochrony danych.
3. Administrator przeprowadza analizy ryzyka naruszenia praw osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter i zakres jak również cele przetwarzania, ryzyko naruszenia praw osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w szczególności ze względu na rodzaj i charakter przetwarzanych danych.
4. Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym celu Administrator ustala przydatność i stosuje takie środki i podejście, jak:
    a. pseudonimizacja,
    b. szyfrowanie danych osobowych,
    c. inne środki, składające się na zdolność do ciągłego zapewniania poufności, integralności, dostępności i adekwatności działalności systemów i usług przetwarzania, w tym przede wszystkich systemów informatycznych,
    d. środki zapewnienia ciągłości działania i zapobiegania skutkom awarii systemowych, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, tak aby Administrator mógł zapewnić:
        i. zabezpieczenie przed wyciekiem danych osobowych przetwarzanych przez Administratora,
        ii. możliwość efektywnego korzystania z praw przyznawanych osobom fizycznym przez RODO (art. 15-22 RODO).

4.9.1. Oceny skutków dla ochrony danych

Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka (stanowiącą załącznik do RCPD), ryzyko naruszenia praw i wolności osób jest wysokie.

4.9.2. Środki bezpieczeństwa podejmowane przez Administratora

Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka, właściwych dla poszczególnych kategorii przetwarzania danych jak również adekwatności podejmowanych środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa przez Administratora.

4.9.3. Raportowanie naruszeń

Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia jak również zawiadomienie osoby, której dane osobowe przetwarzane przez Administratora zostały naruszone, tak by zainteresowana osoba mogła podjąć niezbędne kroki w celu ochrony swoich praw.

4.10. PODMIOTY PRZETWARZAJĄCE DANE OSOBOWE (TZW. „PROCESORY" LUB „PODMIOTY PRZETWARZAJĄCE")

Administrator posiada zasady doboru i weryfikacji podmiotów przetwarzających dane osobowe na rzecz i w imieniu Administratora. Przedmiotowe zasady i procedury zostały opracowane w celu zapewnienia, aby przetwarzający zapewniali gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze, w sposób o którym stanowią postanowienia RODO, dostosowany jednocześnie do specyfiki Administratora tak, by jak najskuteczniej chronić przetwarzane dane osobowe.

Administrator przyjął odpowiednie wymagania co do umowy powierzenia przetwarzania danych, która stanowi Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych".

Administrator rozlicza przetwarzających z wykorzystania podwykonawców przetwarzania danych osobowych, jak też z innych wymagań wynikających z zasad powierzenia danych osobowych. W tym celu Administrator nakłada na podmioty przetwarzające obowiązki przestrzegania reguł bezpieczeństwa u podwykonawców przetwarzania w zakresie w jakim mowa o nałożeniu na te podmioty dokładnie takich samych wymagań faktycznych i prawnych jak na podmioty przetwarzające dane osobowe w imieniu administratora.

4.11. PRZESYŁANIE DANYCH DO PAŃSTW TRZECICH

Administrator rejestruje w RCPD przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2018 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).

Aby uniknąć sytuacji nieautoryzowanego eksportu danych do państw trzecich, w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych, Administrator okresowo weryfikuje zachowania użytkowników.

4.12. PROJEKTOWANIE PRYWATNOŚCI

Administrator w sposób aktywny reaguje na zmiany w zakresie przetwarzania danych osobowych, które mają lub mogą mieć wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

W tym celu zasady prowadzenia projektów i przedsięwzięć przez Administrator odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych. Administrator planując nowe projekty, uwzględnia bezpieczeństwo i minimalizację przetwarzania danych od początku projektu.

5. Klasyfikacja dokumentów

Ten dokument jest sklasyfikowany jako "dokument wewnętrzny Administratora" i nie powinien być ujawniany na zewnątrz firmy bez formalnej zgody zarządu Administratora.

5.1. Własność, aktualizacja i przegląd

Niniejsza Polityka Ochrony Danych Osobowych i Bezpieczeństwa Systemu Informacji jest własnością Administratora. Aktualizacja tego dokumentu jest wykonywana przez zarząd Administratora lub osoby do tego upoważnione.