POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH
w APEX-THERMO KING SP. Z O.O.

80-298 Gdańsk , ul. Geodetów 18, NIP 585-140-89-79

§ 1. Postanowienia ogólne :

1. Niniejszy dokument zawiera opis zasad, obowiązków prawnych oraz procesów i środków które mają wpływ na bezpieczeństwo danych przetwarzanych w przedsiębiorstwie Apex-Thermo King Sp. z o.o. .

2. Zakresem stosowania polityki objęty jest w szczególności Zarząd Apex –Thermo King Sp. z o.o. działający także jako Administrator Danych Osobowych lub jako Podmiot Przetwarzający, oraz osoby przetwarzające dane działające na podstawie stosownych upoważnień.

3. Za nadzór, wprowadzanie zmian i aktualizację polityki odpowiedzialny jest Zarząd Apex -Thermo King Sp. z o.o. Za realizację założeń polityki odpowiedzialne są wszystkie osoby wskazane w polityce.

4. Apex - Thermo King Sp. z o.o. przetwarza dane i informacje zgodnie z wymogami następujących aktów prawnych:

   a. Rozporządzenia Parlamentu Europejskiego i Rady UE nr 2016/679 z dnia 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 96/46/WE (ogólne rozporządzenie o ochronie danych);

   b. Ustawy z dnia 10 maja 2018 r. o ustawie ochrony danych osobowych;

   c. Innych aktów prawnych do których stosowania zobowiązany jest Apex –Thermo King Sp. z o.o. jako podmiot prowadzący działalność gospodarczą na terenie Unii Europejskiej.

§ 2. Definicje.

Ilekroć w niniejszej polityce używa się poniższych terminów i definicji, oznaczają one:

Polityka Bezpieczeństwa Informacji – Polityka Bezpieczeństwa Informacji dotycząca przetwarzania danych osobowych w Apex -Thermo King Sp. z o.o.

Przetwarzanie danych –operacje lub zestaw operacji wykonywanych na danych lub zestawach danych (w tym danych osobowych) w sposób zautomatyzowany lub niezautomatyzowany, takie jak : zbieranie, utrwalania, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, archiwizowanie, usuwanie lub niszczenie.

System informatyczny –zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Infrastruktura teleinformatyczna - Serwery i urządzenia teleinformatyczne; okablowanie służące transmisji danych; stacje Robocze włączone do sieci komputerowej; urządzenia telekomunikacyjne;

Sieć Komputerowa (SK) - Infrastruktura teleinformatyczna wraz ze świadczonymi za jej pomocą usługami;

Stacja Robocza (SR) – komputer osobisty przeznaczony do bezpośredniej pracy;

Użytkownik SR - osoba przejmująca w użytkowanie stację roboczą poprzez podpisanie protokołu odbioru

Zabezpieczenie danych w systemie informatycznym –wdrożenie i stosowanie środków technicznych i organizacyjnych zapewniających ochronę danych przed ich przypadkowym lub nielegalnym zniszczeniem, utratą, modyfikacją, niedozwolonym ujawnieniem lub dostępem, jak również przed wszelkimi nielegalnymi formami ich przetwarzania.

Administrator Danych - osobę fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający –osobę fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane w imieniu administratora.

Podmiot danych – osoba, której dane dotyczą.

Zautomatyzowane podejmowanie decyzji – dokonanie oceny czynników osobowych w procesie automatycznego przetwarzania danych, bez udziału człowieka.

Obowiązek informacyjny – spełnienie przez Administratora Danych wobec podmiotu danych obowiązku poinformowania o zasadach przetwarzania danych osobowych w konkretnej sytuacji, z uwzględnieniem wszystkich informacji których podania wymagają przepisy RODO.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, podlegające ochronie w rozumieniu RODO.

Administrator Danych Osobowych : Zarząd Apex -Thermo King Sp. z o.o.

ADMIKOM (Administrator Systemów Informatycznych) – pracownik wewnętrznego działu IT bądź zewnętrzny usługodawca świadczący wsparcie IT na podstawie odrębnych umów.

Osoba upoważniona (użytkownik) – osoba posiadająca upoważnienie nadane przez ADO do przetwarzania danych osobowych w zakresie w nim wskazanym.

RODO – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady UE nr 2016/679 z dnia 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 96/46/WE (ogólne rozporządzenie o ochronie danych).

§ 3. Zasady przetwarzania danych osobowych

1. Administrator Danych Osobowych przetwarza dane zgodnie z poniższymi zasadami :

   1.1. **Rzetelności i legalności** – co oznacza, że dane przetwarzane będą uczciwie, zgodnie z prawidłowo zidentyfikowanymi, zgodnymi z RODO podstawami prawnymi, adekwatnymi dla poszczególnych czynności przetwarzania. Administrator Danych Osobowych identyfikuje i określa właściwą dla poszczególnej czynności przetwarzania podstawę prawną.

2. **Przejrzystości** – co oznacza, że podmioty danych są w sposób przejrzysty, przystępny i zrozumiały informowane o tym kto, na jakiej podstawie, w jakim celu, w jakim zakresie i jak długo będzie przetwarzała ich dane. Podmioty danych są ponadto informowane o : odbiorcach danych, przysługujących im prawach i sposobie ich realizacji oraz o tym, czy dane będą przekazywane do krajów znajdujących się poza UE i czy dane będą podlegały zautomatyzowanemu podejmowaniu decyzji i jeśli tak, jaki będzie to miało wpływ na sytuację podmiotu danych. Administrator Danych Osobowych zapewnia, że obowiązek informacyjny spełniany będzie :

a. W przypadku zbierania danych od osoby, której dane dotyczą – najpóźniej w momencie ich zbierania,

b. W przypadku zbierania danych z innego źródła niż od osoby, której dane dotyczą – najpóźniej w ciągu 30 dni od ich pozyskania

3. **Ograniczenia celu** – co oznacza, że dane osobowe są zbierane i przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz że nie są przetwarzane dalej w sposób niezgodny z tymi celami.

4. **Minimalizacji danych** – co oznacza, że dane są adekwatne i ograniczone do tego, co niezbędne by osiągnąć cel, dla którego są przetwarzane.

5. **Prawidłowości** – co oznacza, że przetwarzane dane są poprawne, zgodne z prawdą a w razie potrzeby podlegają uaktualnianiu.

6. **Ograniczenia przechowywania** – co oznacza, że dane będą przechowywane w sposób umożliwiający identyfikację podmiotu danych przez okres nie dłuższy, niż jest to niezbędne do realizacji celów, dla których te dane są przetwarzane.

7. **Integralności i poufności** – co oznacza, że dane są przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo a w szczególności w sposób zapewniający ochronę przed : przypadkową lub nieautoryzowaną utratą, modyfikacją, uszkodzeniem lub zniszczeniem. Administrator Danych Osobowych zapewnia bezpieczeństwo danych poprzez stosowanie adekwatnych środków technicznych i organizacyjnych. Administrator Danych Osobowych opracuje system ochrony danych osobowych z uwzględnieniem zdefiniowanych w jego organizacji ryzyk, na które narażone są przetwarzane dane ***(risk based approach***). Opis zastosowanych środków zawarty jest w niniejszym dokumencie.

8. **Rozliczalności** – co oznacza, że Administrator Danych Osobowych przetwarza dane osobowe w sposób gwarantujący przestrzeganie przepisów RODO w związku z operacjami ich przetwarzania oraz, że będzie w stanie wykazać wdrożenie środków organizacyjnych i technicznych zapewniających przetwarzanie danych zgodnie z obowiązującymi przepisami prawa. Wykazanie wdrożenia tych środków odbywać się będzie w szczególności poprzez wdrożenie odpowiednich zasad, procedur i polityk opisujących zasady postępowania przy przetwarzaniu danych.
   Administrator Danych Osobowych dąży do tego, aby każdy proces, rozwiązanie czy pomysł biznesowy, już w fazie jego projektowania był przeanalizowany pod kątem wykorzystania w tym rozwiązaniu danych osobowych i uwzględniał ochronę tych danych. Analiza ta powinna być prowadzona dalej, także już w trakcie samego procesu przetwarzania (***privacy by design***)

§ 4 Dokumentacja

W celu realizacji obowiązków prawnych oraz w celu zapewnienia zasady rozliczalności, Apex -Thermo King Sp. z o.o. prowadzi :

1. Jako Administrator Danych Osobowych - rejestr czynności przetwarzania, zgodny z przepisami zawartymi w RODO. Rejestr ten podlega bieżącej aktualizacji poprzez

odnotowywanie w nim wszelkich zmian, jakie zachodzą w obszarze przetwarzania danych osobowych dla których jest Administratorem Danych.

2. Jako Podmiot Przetwarzający - rejestr kategorii czynności przetwarzania, zgodny z przepisami RODO. Rejestr ten podlega bieżącej aktualizacji poprzez odnotowywanie w nim wszelkich zmian jakie zachodzą w obszarze przetwarzania danych osobowych, które przetwarza jako Podmiot Przetwarzający na zlecenie sowich klientów.
3. Jako Administrator Danych Osobowych – rejestr naruszeń zgodny z przepisami zawartymi w RODO. Rejestr ten podlega aktualizacji w przypadku stwierdzenia naruszenia ochrony danych osobowych.
4. Wzory rejestrów o których mowa w pkt 1-3 stanowią załącznik nr 1 do niniejszej polityki.
5. W celu zapewnienia ochrony dla danych (w tym danych osobowych) Zarząd Apex -Thermo King Sp. z o.o. będzie na bieżąco opracowywał i wdrażał inne dokumenty (procedury, instrukcje, komunikaty i zalecenia).

§ 5 Zarządzanie infrastrukturą teleinformatyczną

5.1 Zarządzanie oprogramowaniem użytkownika końcowego

1. Opiekę informatyczną nad siecią komputerową sprawuje ADMIKOM.
2. Na SR dozwolone i możliwe jest używanie wyłącznie oprogramowania przydzielonego do danej SR przez Administratora IT. O przydziale oprogramowania decyduje ADMIKOM, w porozumieniu z Zarządem spółki. Oprogramowanie musi być użytkowane zgodnie z posiadanymi przez spółkę licencjami, w zakresie ich ilości, wersji i tytułów oraz na warunkach określonych w umowach licencyjnych.
3. Za przechowywanie nośników instalacyjnych i licencji odpowiedzialny jest ADMIKOM danej spółki.
4. Zabrania się dokonywania modyfikacji, usuwania lub kopiowania oprogramowania zainstalowanego na SR. Usunięcie niedozwolonego oprogramowania zainstalowanego na SR nie wymaga wcześniejszego uzyskania akceptacji Użytkowników SR i/lub ich przełożonych.

5.2 Sprzęt komputerowy – zasady przydziału i użytkowania

1. Opiekę nad sprzętem IT użytkowanym przez pracowników oraz Spółki oraz nad serwerami, urządzeniami sieciowymi i innym sprzętem związanym z utrzymaniem infrastruktury IT sprawuje ADMIKOM w porozumieniu z Zarządem. ADMIKOM prowadzi ewidencję sprzętu komputerowego.
2. Sprzęt komputerowy jest przydzielany użytkownikom na wniosek ich bezpośredniego przełożonego, złożony do Administratora IT drogą mailową.
4. Bezpośredni przełożony pracownika, który powinien zostać wyposażony w sprzęt komputerowy, ma obowiązek złożyć w tym zakresie zgłoszenie drogą mailową, najpóźniej na pięć dni roboczych przed rozpoczęciem pracy przez nowego pracownika lub przed przewidywaną wymianą sprzętu u obecnego pracownika.
5. Zgłoszenie o którym mowa w pkt. 4 powinno zawierać :
   a. imię , nazwisko, stanowisko, dział, nr telefonu pracownika,
   b. określenie dostępów.
6. Każdy pracownik, któremu przyznano SR do celów służbowych ma obowiązek pokwitować jego odbiór na protokole zdawczo-odbiorczym. Rejestr protokołów prowadzi ADMIKOM.
7. Osoby użytkujące przenośny komputer zobowiązane są zachować szczególną ostrożność podczas transportu i przechowywania komputera. Do korzystania z firmowego komputera przenośnego upoważniona jest wyłącznie osoba będąca pracownikiem Spółki.
8. Za zabezpieczenie komputera przenośnego przed kradzieżą, uszkodzeniem lub zniszczeniem odpowiedzialny jest Użytkownik SR.
9. Każda utrata firmowego komputera przenośnego, bezwzględnie wymaga zgłoszenia faktu kradzieży na Policję oraz poinformowania Administratora IT oraz Zarządu.
10. Wszystkie dane firmowe (w tym dane osobowe) muszą być przechowywane w wyznaczonych katalogach sieciowych, dedykowanych i zatwierdzonych do użytkowania aplikacjach. Przypadek utraty danych przechowywanych na SR, bez kopii znajdującej się w katalogach sieciowych lub dedykowanych aplikacjach (np. w przypadku awarii dysku lub też kradzieży sprzętu), będzie rodził odpowiedzialność porządkową pracowników, a w przypadku szkody w mieniu pracodawcy pracownik poniesie odpowiedzialność za szkodę, zgodnie z przepisami Kodeksu pracy.
11. Zabrania się umieszczania w katalogach sieciowych jakichkolwiek plików prywatnych (zdjęć, filmów, itp.). Zabrania się przechowywania w SK jakichkolwiek plików naruszających prawa autorskie. W/w pliki mogą zostać usunięte bez konieczności uzyskania zgody Użytkownika SK i/lub jego przełożonych.
12. W przypadku opuszczenia stanowiska pracy, Użytkownik SK zobowiązany jest do wylogowania się lub zablokowania SR.
13. Zabrania się samodzielnego działania w zakresie rozbudowy i wprowadzania zmian w użytkowanym sprzęcie komputerowym oraz ingerencji w okablowanie strukturalne.

14. Wszelkie zmiany w konfiguracji SR wykonuje ADMIKOM na podstawie zgłoszonych potrzeb i uzgodnień dokonanych z Zarządem.
15. Zgłoszenie dotyczące odejścia pracownika musi być zgłoszone w formie e-mailowej i winno obejmować informacje dot. przekierowania poczty elektronicznej ze wskazaniem osób, które powinny obsługiwać pocztę po odchodzącym pracowniku, oraz informacje odnośnie sposobu archiwizacji zasobów dysku domowego po odchodzącym pracowniku.
16. Zgłoszenie dotyczące odejścia pracownika winno obejmować informacji o terminie i miejscu zdania używanej przez odchodzącego pracownika SR. SR powinna być zdana do Administratora IT najpóźniej w ostatnim dniu obecności w pracy.
17. Zgłoszenie dotyczące odejścia pracownika powinno zostać złożone najpóźniej w ostatnim dniu pracy osoby odchodzącej.

5.3 Zarządzanie pojemnością i wydajnością komponentów infrastruktury

1. Za zarządzanie pojemnością i wydajnością komponentów infrastruktury teleinformatycznej odpowiedzialny jest ADMIKOM.

2. ADMIKOM dokonuje cyklicznych przeglądów wszystkich komponentów infrastruktury teleinformatycznej. Przeglądy nie powinny odbywać się rzadziej niż 1 raz w roku kalendarzowym.

3. Podczas przeglądu komponentów infrastruktury, brane są pod uwagę w szczególności następujące kryteria :

   a. Wydajność (np. czas odpowiedzi systemu, czas przetwarzania) wraz ze wskazaniem wartości ostrzegawczych i granicznych w tym zakresie;

   b. Pojemność (np. obciążenie sieci teleinformatycznej, stopień wykorzystania urządzeń pamięci masowych, stopień wykorzystania procesorów, liczba otwartych sesji połączeniowych), wraz ze wskazaniem wartości ostrzegawczych i granicznych w tym zakresie

   c. Stopień zużycia wraz ze wskazaniem wartości ostrzegawczych i granicznych w tym zakresie.

4. ADMIKOM na wniosek Zarządu ma obowiązek sporządzenia raportu z przeprowadzonego przeglądu. Raport jest składany do Zarządu i powinien uwzględniać w szczególności :

   a. wynik testu wydajności,

   b. wynik testu pojemności,

c. określenie stopnia zużycia,

d. zasady monitorowania parametrów określonych w punktach a, b, c

e. wskazanie trendów i prognoz zapotrzebowania na wydajność i pojemność w związku z wyznaczonymi celami strategicznymi Przedsiębiorstwa

f. rekomendacje działań w przypadku przekroczenia wartości ostrzegawczych i granicznych powyższych parametrów oraz w przypadku, gdy analizy w zakresie zapotrzebowania na wydajność i pojemność wykażą, że obecne zasoby nie są wystarczające do jego zaspokojenia.

5.4. Odpowiedzialność za poszczególne obszary zarządzania strukturą teleinformatyczną

1. Osobą odpowiedzialną za zarządzanie, monitorowanie i bieżący nadzór nad strukturą teleinformatyczną jest ADMIKOM.
2. Do obowiązków ADMIKOM należy w szczególności :
   a. budowa, udoskonalanie i zarządzanie strukturą teleinformatyczną,
   b. zarządzanie płynnością pracy w sieci teleinformatycznej,
   c. monitorowanie prawidłowości działania systemów,
   d. zarządzanie uprawnieniami dostępu dla użytkowników,
   e. nadzór nad serwerami, urządzeniami sieciowymi, oraz komputerami użytkowników,
   f. testowanie prawidłowości tworzenia kopii zapasowych,
   g. wsparcie dla użytkowników,
   h. współpraca z zewnętrznymi dostawcami usług wspierającymi pracę sieci teleinformatycznej,
   i. nadzór nad obszarem bezpieczeństwa teleinformatycznego.

3. ADMIKOM prowadzi działania naprawcze, monitorujące i inicjujące udoskonalanie w obszarze funkcjonowania i bezpieczeństwa infrastruktury teleinformatycznej poprzez:
   a. Bieżące prowadzenie analizy ryzyka w obszarze bezpieczeństwa środowiska teleinformatycznego,
   b. Zarządzanie incydentami bezpieczeństwa teleinformatycznego,
   c. Raportowanie Zarządowi wyników analizy bezpieczeństwa oraz informacji o stwierdzonych incydentach, sposobie postępowania z nimi oraz zastosowanych środkach zapobiegających incydentom na przyszłość.

5.5. Współpraca z zewnętrznymi dostawcami usług

1. Wyboru zewnętrznych dostawców usług wspierających funkcjonowanie systemu IT, dokonuje się z zachowaniem należytej staranności i przy uwzględnieniu zawodowego charakteru działalności w ramach świadczonych przez dostawcę usług.
2. Ostatecznego wyboru dostawcy usług dokonuje Zarząd, po przedstawieniu wniosku zaopiniowanego przez ADMIKOM.
3. Nawiązanie współpracy z zewnętrznym dostawcą usług, w ramach której występuje konieczność udostępnienia danych osobowych dla celów niezbędności realizacji umowy z dostawcą , bezwzględnie wymaga zawarcia pisemnej umowy o powierzenie do przetwarzania danych osobowych. Zakres informacji jakie obowiązkowo musi zawierać umowa o powierzenie, określa § 7 pkt 5 niniejszej polityki.
4. Umowy z dostawcami usług zewnętrznych powinny ponadto określać w szczególności :
   a. zakresy odpowiedzialności stron umowy,
   b. zakres informacji i dokumentacji przekazywanych przez usługodawcę w związku ze świadczeniem usług,
   c. zasady wymiany i ochrony informacji, w tym warunki nadawania pracownikom podmiotów zewnętrznych praw dostępu do informacji oraz zasobów środowiska teleinformatycznego,
   d. zasady odpowiedzialności za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu umowy,
   e. zasady związane z prawami do oprogramowania (w tym jego kodów źródłowych) w trakcie współpracy i po jej zakończeniu, w szczególności dostępu do kodów źródłowych w przypadku zaprzestania świadczenia usług wsparcia i rozwoju oprogramowania przez jego dostawcę,
   f. parametry dotyczące jakości świadczonych usług oraz sposoby ich monitorowania i egzekwowania,
   g. zasady i tryb obsługi zgłoszeń dotyczących problemów w zakresie świadczonych usług,
   h. zasady i tryb dokonywania aktualizacji oprogramowania komponentów infrastruktury znajdujących się pod kontrolą dostawcy (jeśli dotyczy),
   i. zasady współpracy w przypadku wystąpienia incydentu naruszenia bezpieczeństwa środowiska teleinformatycznego (jeśli dotyczy),
   j. zasady w zakresie dalszego zlecania czynności podwykonawcom zewnętrznego dostawcy usług,
   k. kary umowne związane z nieprzestrzeganiem warunków umownych, w szczególności w zakresie bezpieczeństwa informacji przetwarzanych przez dostawcę usług

§ 6. Środki techniczne i organizacyjne zapewniające ochronę i bezpieczeństwo danych (w tym danych osobowych).

6.1. Opis stosowanych technicznych środków bezpieczeństwa

1. Wszelkie dane, w tym dane osobowe, przetwarzane w przedsiębiorstwie zabezpieczane są w sposób zapewniających ich poufność, dostępność i integralność, przy uwzględnieniu: aktualnego stanu wiedzy technicznej, kosztów wdrażania rozwiązań technicznych a także charakteru, zakresu, kontekstu i celów przetwarzanych danych.
2. Szczegółowy opis środków i metod technicznych stosowanych w celu zapewnienia bezpieczeństwa znajduje się w pkt. 6.5 niniejszej polityki – *6.4. Instrukcja zarządzania systemem informatycznym*

6.2. Opis stosowanych organizacyjnych środków bezpieczeństwa

Administrator Danych Osobowych stosuje następujące, organizacyjne środki bezpieczeństwa :

1. Dostęp do pomieszczeń biurowych w których odbywa się przetwarzania jest chroniony przed dostępem osób niepowołanych, poprzez stanowisko recepcji, której pracownicy uniemożliwiają
   wejście do pomieszczeń w których przetwarzane są dane osobowe, osobom niepowołanym.
2. Osoby odwiedzające biuro są przyjmowane przez pracowników biura i pytane o cel wizyty, wstęp do pomieszczeń tylko po imiennym wskazaniu osoby, która ma prawo przebywać w pomieszczeniach biurowych.
3. Goście odwiedzający biuro są przyjmowani w wyznaczonych salach, bez żadnego dostępu do dokumentów oraz urządzeń, na którym możliwy jest dostęp do danych osobowych, za które odpowiada Administrator Danych Osobowych.
4. Pracownicy i osoby współpracujące stosują zasadę „czystego biurka” – po zakończeniu dnia pracy wszystkie dokumenty zawierające dane osobowe musza być schowane do zamykanych biurek lub szuflad. Dokumenty robocze, nie podlegające archiwizacji musza być niszczone na bieżąco poprzez ich pocięcie w niszczarce, najpóźniej na koniec każdego dnia pracy.
5. Każda osoba dopuszczona do przetwarzania danych otrzymuje upoważnienie do przetwarzania, z wskazaniem zakresu i czynności przetwarzania, do których nadano upoważnienie. Wzór upoważnienia stanowi załącznik 2 do niniejszej polityki.
6. Każda osoba upoważniona do przetwarzania zostaje zobowiązana do zachowania poufności oraz do utrzymania w tajemnicy informacji, które pozyska w związku z przetwarzaniem – podpisując w tym zakresie oświadczenie, którego wzór stanowi załącznik nr 3 do niniejsze polityki.
7. Administrator Danych Osobowych prowadzi rejestr osób upoważnionych, który na bieżąco aktualizuje. Wzór rejestru stanowi załącznik nr 4 do niniejszej polityki.
8. Monitory ustawione są w sposób uniemożliwiający wgląd osobom nieupoważnionym.

9. Dokumenty kadrowe i zawierające dane poufne przechowywane są w metalowej, zamykanej na klucz szafie do której dostęp mają jedynie osoby upoważnione. Szafa znajduje się w odizolowanym od osób nieuprawnionych miejscu.

6.3. Analiza ryzyka i analiza skutków dla ochrony danych

1. Stosując zasadę *risk based approach* Administrator Danych Osobowych zobowiązany jest przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
2. W przypadku, gdy w przedsiębiorstwie Administratora planowany jest rodzaj przetwarzania, w szczególności z użyciem nowych technologii, który ze względu na swój charakter, kontekst, zakres i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, przed wdrożeniem tego rodzaju przetwarzania przeprowadzona zostanie analiza skutków dla ochrony danych.
3. W szczególności analiza skutków dla ochrony danych będzie przeprowadzona w sytuacji, gdy planowana czynność przetwarzania znajdować się będzie w wykazie czynności wymagających przeprowadzenia analizy skutków, opublikowanym przez Prezesa Urzędu Ochrony Danych w Monitorze Polskim.
4. Przyjęto, że analiza ryzyka oraz ewentualna ocena skutków dla ochrony danych przeprowadzana jest dla procesów (czynności przetwarzania).
5. Analiza ryzyka oraz analiza skutków prowadzona jest przy użyciu dostępnych metod pozwalających w sposób adekwatny i wiarygodny oszacować ryzyko dla danych osobowych przetwarzanych w przedsiębiorstwie. Wynik przeprowadzonej analizy ryzyka stanowi integralną część niniejszej polityki.
6. Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np., nowe czynności przetwarzania, zmiany prawne, nowe systemy, poważne incydenty, zmiana wykazu czynności wymagających przeprowadzenia oceny skutków).
7. Na podstawie przeprowadzonej analizy ryzyka, Administrator Danych Osobowych podejmuje decyzje odnośnie obniżenia bądź akceptacji istniejących ryzyk. W przypadku decyzji o obniżeniu ryzyka, Administrator Danych Osobowych sporządza listę zabezpieczeń do wdrożenia, wyznaczając jego termin i osoby odpowiedzialne.

6.4. Instrukcja zarządzania systemem informatycznym

1. **Realizację zamierzeń określonych w niniejszym punkcie gwarantuje następująca strategia:**
   a. Przeszkolenie użytkowników w zakresie ochrony danych osobowych oraz zaznajomienie z przepisami dotyczącymi ochrony danych osobowych,
   b. korzystanie z adekwatnego co do możliwości przedsiębiorstwa oraz ilości przetwarzanych w nim danych osobowych, oprogramowania systemowego i użytkowego,
   c. Zaimplementowanie w systemie informatycznym aktualnych zabezpieczeń gwarantujących nienaruszoną pracę systemu,
   d. Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła i identyfikatory),
   e. Ocena ewentualnych zagrożeń bezpieczeństwa systemu informatycznego i ryzyka związanych z jego obsługą,
   f. Monitorowanie wdrożonych zabezpieczeń w celu identyfikacji podatnych na zagrożenia obszarów i słabości zabezpieczeń,
   g. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych oraz podejmowanie niezbędnych działań dla likwidacji słabych ogniw w systemie zabezpieczeń w ramach przeglądów bezpieczeństwa.

2. **Metody i środki uwierzytelniania**

   a. Mając na względzie, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych, dla każdej osoby upoważnionej ustalany jest odrębny identyfikator i hasło, tak, aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym

   mógł mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
   b. Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników.
   c. Hasła znane są tylko właścicielowi (użytkownikowi).
   d. Identyfikator użytkownika:
   • jest niepowtarzalny,
   • po wyrejestrowaniu użytkownika z systemu informatycznego Przedsiębiorstwa nie jest przydzielany innej osobie,
   • nie podlega zmianie,
   • użytkownicy zobowiązani są do zachowania w tajemnicy ustalonych dla nich

identyfikatorów,
• jest wpisywany do ewidencji osób upoważnionych wraz z imieniem i nazwiskiem użytkownika oraz jest rejestrowany w systemie przetwarzającym dane osobowe.
e. Hasło użytkownika:
• jest ustalane indywidualnie przez każdego z użytkowników i znane tylko użytkownikowi, który się nim posługuje,
• nie jest zapisywane w systemie w postaci jawnej,
• jest zmieniane **co 42 dni,**
• nie może zawierać nazwy konta użytkownika ani części jego pełnej nazwy dłuższej niż dwa kolejne znaki.

• musi zawierać znaki z trzech spośród następujących czterech kategorii:

1) Wielkie litery alfabetu łacińskiego (od A do Z)

2) Małe litery alfabetu łacińskiego (od a do z)

3) Cyfry systemu dziesiętnego (od 0 do 9)

4) Znaki niealfabetyczne (na przykład !, $, #, %)

• składa się co najmniej z 7 znaków, duże i małe litery, cyfra, znak specjalny,

f. Niezależnie od wymogu zmieniania haseł, hasło powinno być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie.
g. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy wykorzystaniu hasła, którym się posługuje lub posługiwał.

h. Użytkownik obowiązany jest utrzymywać hasła, którymi się posługuje lub posługiwał, w ścisłej tajemnicy, co obejmuje w szczególności dołożenie przez niego wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem nawet po ustaniu jego ważności, czy też wykrycia hasła przez te osoby.
i. W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić

o tym Administratora Danych.
j. Niedopuszczalna jest praca w systemie informatycznym przy użyciu identyfikatora innego użytkownika.
k. Naruszenie przez użytkownika postanowień punktu 2 podpunkt h-j może stanowić podstawę

dla pociągnięcia użytkownika do odpowiedzialności dyscyplinarnej.

3. Zarządzanie uprawnieniami do systemu informatycznego

a. Uprawnienia do systemu informatycznego nadawane są przez osobę wyznaczoną przez Administratora Danych i odpowiedzialną za zarządzanie systemem informatycznym, na podstawie zgłoszenia bezpośredniego przełożonego osoby mającej uzyskać uprawnienia. Dopuszcza się przekazanie zgłoszenia poprzez wysłanie wiadomości e-mail do osoby odpowiedzialnej za zarządzanie systemem informatycznym

b. Dana osoba jest rejestrowana w systemie informatycznym jako użytkownik po spełnieniu następujących warunków:

   • uzyskaniu przez tą osobę — upoważnienia wydanego przez Administratora Danych dopuszczającego daną osobę w zakresie w nim wskazanym jako użytkownika do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych,

   • odbycia wstępnego przeszkolenia w zakresie bezpiecznego korzystania z systemu informatycznego oraz w zakresie ochrony danych osobowych przetwarzanych w Przedsiębiorstwie.

c. Użytkownik jest wyrejestrowywany (konto jest blokowane) z systemu informatycznego w przypadku zakończenia lub zawieszenia współpracy z osobą upoważnioną, co równoznaczne jest z odwołaniem przez Przedsiębiorstwo wydanego temu użytkownikowi upoważnienia.

d. Identyfikator, który utracił ważność, nie może być ponownie przydzielony innemu użytkownikowi.

4. Rozpoczęcie, zawieszenie i zakończenie pracy

a. Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych służących do przetwarzania danych z uwzględnieniem, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

b. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu informatycznego, każdy pracownik zobowiązany jest poinformować o tym Administratora Danych oraz nie rozpoczynać pracy do czasu jego interwencji oraz zadeklarowania bezpieczeństwa stanowiska pracy.

c. Każdy użytkownik rozpoczynając pracę obowiązany jest zalogować się do systemu komputerowego Przedsiębiorstwa posługując się swoim identyfikatorem i hasłem, dokładając jednocześnie szczególnej staranności w tym, aby przy tych czynnościach osoby trzecie nie powzięły wiadomości o treści używanego przez niego hasła.

d. Przed opuszczeniem miejsca pracy użytkownik obowiązany jest wylogować się z systemu oraz zablokować komputer.

e. Kończąc pracę użytkownik obowiązany jest wylogować się z systemu informatycznego, zablokować lub zamknąć system operacyjny oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji. Opuszczając stanowisko użytkownik zamyka używane przez niego szafy i pomieszczenia, w których przechowuje się dokumentację Przedsiębiorstwa i nośniki informacji.

5. Ogólny opis stosowanych zabezpieczeń sieci informatycznej.

a. Stacje robocze na których odbywa się przetwarzanie danych osobowych, są zabezpieczone oprogramowaniem AV. Instalowane jest na nich jedynie legalne oprogramowanie, które podlega aktualizacjom wg wymagań producenta oprogramowania.

b. Kopie zapasowe dla dysków sieciowych tworzone są według ustalonego harmonogramu – **pełna kopia zapasowa wykonywana w każda sobotę, natomiast codziennie są wykonywane kopie przyrostowe.**

c. Kopie zapasowe danych przechowywane są na osobnym urządzeniu.

d. Serwery chronione są oprogramowaniem AV.

e. Wewnętrzna sieć **serwerowa** chroniona jest przed zagrożeniami płynącymi z połączeniem z siecią publiczna **urządzaniem** typu firewall.

f. Dostęp do pomieszczeń serwerowni jest ściśle ograniczony, chroniony zamkiem cyfrowym i możliwy tylko dla wyznaczonych osób.

g. Pomieszczenie serwerowni wyposażone w system klimatyzacji, oraz w systemy UPS podtrzymujące zasilanie.

h. Wydzielono odrębne pasmo Wi-Fi przeznaczone dla osób trzecich, bez możliwości połączenia z zasobami informatycznymi Przedsiębiorstwa.

i. Zastosowano szyfrowaną transmisję danych (VPN).

j. Nie rzadziej niż raz na rok wykonywane są okresowe czynności testujące prawidłowość zapisu i możliwości odczytu danych z utworzonych kopii zapasowych.

k. Nie rzadziej niż raz na rok Administrator dokonuje przeglądu stosowanych zabezpieczeń i w razie potrzeby dokonuje stosownych korekt w tym zakresie.

6. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków

a. Wydruki komputerowe są bezzwłocznie usuwane po ustaniu ich użyteczności, czego dokonać należy poprzez zniszczenie ich w sposób trwały, tj. za pomocą niszczarki.

b. Urządzenia, dyski lub inne informatyczne nośniki informacji zawierające dane osobowe przeznaczone do likwidacji podlegają przekazaniu ich do podmiotu wyspecjalizowanego i uzyskanie protokołu potwierdzającego fizyczne zniszczenie nośników. Przed przekazaniem, nośniki informacji zostają pozbawione danych osobowych poprzez ich trwałe usunięcie (nadpisanie i usunięcie metadanych plików).

c. Trwałego zniszczenia zbędnych wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

d. Nośniki danych (inne niż kopie zapasowe) przechowywane są w zamykanych na klucz szafkach lub szufladach po godzinach pracy.

7. Sposób dokonywania przeglądów i konserwacji systemu oraz nośników informacji

a. Przeglądów i konserwacji sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z obciążenia sprzętu komputerowego, warunków zewnętrznych, w których eksploatowane są dane urządzenia oraz ważności sprzętu dla funkcjonowania całości systemu informatycznego Przedsiębiorstwa.

b. W przypadku konieczności naprawy sprzętu poza siedzibą, jest on przekazywany do serwisu po uprzednim wymontowaniu dysku/dysków twardych na których przechowywane są dane osobowe.

8. Sposób postępowania w zakresie komunikacji w sieci komputerowej

a. Komunikacja w sieci komputerowej jest dozwolona jedynie po właściwym zalogowaniu się i podaniu własnego hasła użytkownika.

b. Wprowadzanie do systemu informatycznego informacji z zewnątrz, w tym danych osobowych, jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i tylko przez użytkownika w zakresie jego obowiązków i wynikających z nich uprawnień.

§ 7. Zasady udostępniania i powierzania danych (w tym danych osobowych)

1. Administrator Danych Osobowych udostępnia (w tym powierza) dane osobowe innym podmiotom (odbiorcom danych) na podstawie :

   a. obowiązujących przepisów prawa

   b. decyzji biznesowych dotyczących outsourcingu wybranych części działalności.

2. Do podmiotów upoważnionych z mocy prawa zalicza się podmioty, którym Administrator Danych Osobowych jest zobowiązany udostępniać dane osobowe na podstawie powszechnie obowiązującego prawa. Taki rodzaj udostępnienia nie wymaga złożenia pisemnego wniosku, udostepnienie jest realizowane na podstawie wiedzy o obowiązkach, jakim podlega Administrator Danych Osobowych.

3. Administrator Danych Osobowych, może występować z prośbą o opinię prawną lub ekspercką, w przypadku wątpliwości co do stwierdzenia podstaw upoważniających do udostępnienia danych.

4. W przypadku udostępnienia danych podmiotom, którym Administrator Danych Osobowych zleca wykonanie usług w swoim imieniu i na swoją rzecz, wymagane jest zawarcie umowy o powierzenie do przetwarzania w formie pisemnej.

5. Umowa o powierzenie do przetwarzania musi określać co najmniej :

   a. przedmiot i czas trwania przetwarzania,

   b. charakter i cel przetwarzania,

   c. rodzaj powierzanych danych,

   d. kategorie osób których powierzane dane dotyczą,

   e. obowiązki i prawa Administratora i Podmiotu Przetwarzającego,

   f. decyzję co do sposobu postępowania z powierzonymi danymi po zakończeniu trwania umowy o powierzenie.

6. Każda decyzja dotycząca outsourcingu usług, wymaga przeanalizowania jej przez Administratora Danych Osobowych także pod kątem zawarcia umowy o powierzenie do przetwarzania.

§ 8. Udzielanie informacji osobom, których dane dotyczą

1. Uprawnienia do udzielania informacji podmiotom danych realizowane jest w następujący sposób :

a. Administrator Danych na wniosek każdej osoby której dane osobowe przetwarza, udziela dostępu do jej danych osobowych oraz udziela informacji o :

- celu przetwarzania,
- podstawie prawnej przetwarzania,
- kategoriach odnośnych danych,
- informacji o odbiorcach danych lub kategoriach odbiorców którym dane zostały ujawnione,
- planowanym okresie przechowywania danych osobowych,
- prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
- prawie wniesienia skargi do organu nadzorczego w zakresie ochrony danych osobowych,
- źródle z którego pozyskano dane osoby – w przypadku gdy nie pochodzą one wprost od niej,

b. Określone w punkcie a informacje są zgodnie z realizacja zasady przejrzystości określonej **w § 3 pkt 1 podpunkt 1.2** niniejszej polityki, podawane podmiotom danych w klauzulach informacyjnych.

c. Niezależnie od realizacji obowiązku informacyjnego, podmiot danych ma prawo zwrócić się z wnioskiem o udzielenie informacji odnośnie jej danych osobowych.

d. Wniosek o udostępnienie danych powinien być skierowany na adres mailowy : apextk@apextk.pl bądź złożony osobiście przez wnioskodawcę w siedzibie Administratora Danych Osobowych.

e. Administrator Danych Osobowych przekazuje osobie, która wnioskuje o przekazanie dotyczących jej danych osobowych kopię danych podlegających przetwarzaniu. Za przekazanie kolejnych kopii na wniosek tej samej osoby, Administrator ma prawo pobrać opłatę w rozsądnej wysokości.

f. Administrator Danych Osobowych na wniosek osoby, której dane dotyczą, przekazuje dane osobowe pozyskane od tej osoby, do wskazanego przez nią Administratora Danych o ile dane są przetwarzane na podstawie zgody, lub podstawą do przetwarzania jest zawarcie umowy której stroną jest osoba, której dane dotyczą. Dane podlegające przenoszeniu będą przesłane do wskazanego Administratora w formacie XML bądź PDF.

g. Osoba, której dane są przetwarzane na podstawie udzielonej przez nią zgody ma prawo do cofnięcia tej zgody w każdym czasie. Wniosek o cofnięcie zgody powinien być złożony osobiście w siedzibie Administratora Danych albo w formie elektronicznej w drodze maila skierowanego na adres e-mail: apextk@apextk.pl. Cofnięcie zgody nie ma wpływu na legalność przetwarzania które miało miejsce przed cofnięciem zgody.

h. Administrator Danych Osobowych przeprowadza weryfikację tożsamości osoby składającej wniosek jako podmiot danych. Dąży przy tym do zebrania możliwie najmniejszej ilości informacji, pozwalających na skuteczną weryfikację tożsamości osoby składającej wniosek. Informacje zebrane w celu weryfikacji tożsamości nie są utrwalane.

i. W sytuacji, gdy niemożliwe jest ustalenie tożsamości osoby składającej wniosek, Administrator Danych Osobowych ma prawo odmówić uwzględnienia złożonego wniosku.

j. O dokonanym sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych, Administrator Danych Osobowych poinformuje odbiorców, którym dane zostały przez niego ujawnione chyba, że okazałoby się to niemożliwe lub wymagałoby od Administratora Danych Osobowych niewspółmiernego wysiłku. Przekazanie stosownych informacji do odbiorców danych powinno odbyć się niezwłocznie, nie później jednak niż w ciągu 30 dni od dokonania czynności.

k. Udzielanie odpowiedzi na złożone wnioski i realizacja praw podmiotów danych odbywa się niezwłocznie, nie później niż w ciągu 21 dni od momentu złożenia wniosku o udzielenie informacji o danych osoby które jej dotyczą.

l. Obsługa wniosków podmiotów danych jest prowadzona przez wyznaczonego przez Zarząd i przeszkolonego w tym zakresie pracownika.

§ 9. Retencja danych

1. Dane osobowe przetwarzane w Apex -Thermo King Sp. z o.o. są usuwane zawsze po ustaniu okresu, jaki Administrator przewidział dla ich przetwarzania. Okres ten jest ustalany i podawany przez Administratora Danych Osobowych w rejestrze czynności przetwarzania oraz podawany podmiotom danych w klauzulach informacyjnych.

2. Administrator Danych Osobowych ustala okres retencji danych biorąc pod uwagę w szczególności :

   a. obowiązujące w danym zakresie przepisy prawa nakazujące przechowywać dane przez wskazany okres czasu,

   b. przewidywany okres realizacji celu, dla którego dane są przetwarzane,

   c. okoliczności, w których konieczne będzie wywiązanie się przez Administratora z obowiązku prawnego na mocy prawa krajowego lub unijnego (np. skuteczne dochodzenie roszczeń lub obrona przed nimi, bądź obowiązek okazania dokumentów instytucjom kontrolującym)

3. Dane osobowe powierzone do przetwarzania firmie Apex -Thermo King Sp. z o.o. na podstawie umowy o powierzenie do przetwarzania, są usuwane lub zwracane poszczególnym Administratorom wg zapisów konkretnych umów.

4. Administrator Danych Osobowych, dokonuje nie rzadziej niż 1 raz w roku analizy prowadzonego rejestru czynności przetwarzania w którym określono czas przechowywania danych. Na podstawie tej analizy dokonuje przeglądu zasobów danych osobowych i wydaje ewentualne decyzje o ich usunięciu.

5. Szczegółowe zasady postępowania w związku z retencją danych osobowych określa odrębna procedura.

§ 10. Zasady postępowania w przypadku naruszeń w obszarze ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych lub zobowiązana do zachowania poufności danych osobowych w przypadku stwierdzenia zaistnienia podatności lub wystąpienia incydentu, zobowiązana jest poinformować o tym bezpośredniego przełożonego lub Administratora Danych Osobowych.

2. Do typowych podatności na narażenie bezpieczeństwa danych osobowych należą:

a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek.

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),

c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/ sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych Osobowych prowadzi postępowanie wyjaśniające w toku którego:

    a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

    b. inicjuje ewentualne działania dyscyplinarne,

    c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

    d. dokumentuje prowadzone postępowania.

5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych Osobowych prowadzi postępowanie wyjaśniające w toku którego:

a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

b. zabezpiecza ewentualne dowody,

c. ustala czy i wobec jakiej ilości osób których dane są przetwarzane, mogło dojść do naruszenia ich praw i wolności,

d. zgłasza wystąpienie incydentu do Organu Nadzorczego, zgodnie z obowiązującymi w tym zakresie przepisami, nie później niż w ciągu 72 godzin od momentu wystąpienia incydentu, jeżeli uzna, że incydent taki z dużym prawdopodobieństwem może naruszyć prawa i wolności osób, których dane są przetwarzane,

e. informuje osoby, których dane są przetwarzane o wystąpieniu incydentu jeżeli uzna, że incydent taki z dużym prawdopodobieństwem może naruszyć prawa i wolności osób, których dane są przetwarzane,

f. prowadzi współpracę z Organem Nadzorczym i stosuje się do wydawanych przez niego zaleceń,

g. ustala osoby odpowiedzialne za naruszenie i inicjuje ewentualne działania dyscyplinarne,

h. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),

i. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,

j. dokumentuje prowadzone postępowania.

6. Administrator Danych osobowych prowadzi rejestr naruszeń, którego wzór jest opisany w załączniku nr 1.

7. Administrator Danych Osobowych jest odpowiedzialny za złożenie zawiadomienia o wystąpieniu incydentu do Organu Nadzorczego. Od zgłoszenia takiego Administrator Danych Osobowych może odstąpić wtedy, gdy w toku prowadzonego postępowania wyjaśniającego uzna, że istnieje małe prawdopodobieństwo aby naruszenie mogło wywołać skutki w postaci naruszenia praw i wolności osób, których dane są przetwarzane.

8. Administrator Danych Osobowych jest odpowiedzialny za zawiadomienie osoby której dane osobowe zostały bezprawnie ujawnione, zniszczone bądź zmodyfikowane wskutek wystąpienia incydentu. Jeżeli wysoce prawdopodobne jest, że w wyniku incydentu prawa i wolności osoby nie zostały i nie zostaną naruszone, Administrator Danych Osobowych może odstąpić od zawiadomienia osoby której dane dotyczą.

9. Jeżeli incydent (naruszenie) dotyczą danych osobowych, które zostały powierzone do przetwarzania Apex -Thermo King Sp. z o.o., wówczas zawiadomienie o stwierdzonym incydencie (naruszeniu) dokonywane jest wobec właściwego Administratora Danych w terminie określonym właściwą umową o powierzenie do przetwarzania.

10. Apex -Thermo King Sp. z o.o. działając jako podmiot przetwarzający będzie podejmował wszelkie przewidziane w niniejszym punkcie działania, w celu udzielenia Administratorowi Danych wszelkiej niezbędnej pomocy w ustaleniu zakresu incydentu (naruszenia) i zminimalizowaniu jego skutków.

§ 11. Szkolenia dla osób upoważnionych do przetwarzania danych

Każda osoba, która zostaje upoważniona do przetwarzania danych osobowych w przedsiębiorstwie Apex -Thermo King Sp. z o.o., przed przystąpieniem do wykonania obowiązków zobowiązana jest do zapoznania się z „Polityką bezpieczeństwa danych przetwarzanych w firmie w Apex-Thermo King Sp. z o.o." i złożenia oświadczenia, iż przyjmuje do stosowania zawarte w tym dokumencie treści. W tym przestrzegania zasad bezpieczeństwa w zakresie ochrony danych osobowych obowiązujących w firmie Apex- Thermo King Sp. z o.o.

§ 12 Wejście w życie

Niniejsza procedura wchodzi w życie z dniem jej zatwierdzenia przez Zarząd przedsiębiorstwa Apex -Thermo King Sp. z o.o.