POLITYKA BEZPIECZEŃSTWA INFORMACJI REMARK-KAYSER SPÓŁKA Z O.O. Z SIEDZIBĄ W BATOROWIE

1) Strategia bezpieczeństwa

§ 1. Definicje

1) Użyte w niniejszej Polityce Bezpieczeństwa Informacji pojęcia oznaczają:
   a) Administrator – **REMARK-KAYSER SPÓŁKA Z O.O.** z siedzibą w Batorowie, posiadająca REGON 630689063 oraz NIP 7811095831, z zastrzeżeniem ustępu 2,
   b) pracownik – osoba świadcząca pracę Administratorowi na podstawie stosunku pracy lub innego stosunku prawnego. Zapisy niniejszej Polityki Bezpieczeństwa Informacji odnoszące się do pracowników stosuje się także do stażystów i praktykantów,
   c) trwały nośnik - materiał lub narzędzie umożliwiające przechowywanie informacji, w sposób umożliwiający dostęp do informacji w przyszłości przez czas odpowiedni do celów, jakim te informacje służą, i które pozwalają na odtworzenie przechowywanych informacji w dowolnym czasie w niezmienionej postaci.
2) Przepisy niniejszej Polityki Bezpieczeństwa Informacji mają zastosowanie także wtedy, kiedy Administrator przetwarza dane osobowe jako procesor, któremu powierzono dane do przetwarzania lub podmiot przetwarzający, w rozumieniu odpowiednich przepisów prawa.

§ 2. Cel

Celem wprowadzenia Polityki Bezpieczeństwa Informacji jest:

a) zapewnienie wymaganego zaangażowania pracowników w utrzymanie poziomu bezpieczeństwa informacji w tym ochrony danych osobowych które przetwarza Administrator,
b) określenie kierunków rozwoju zarządzania bezpieczeństwem informacji w tym ochroną danych osobowych, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa oraz zagwarantowaniu sprawnego funkcjonowania Administratora,
c) identyfikowanie i obniżanie ryzyk związanych z bezpieczeństwem informacji, w tym ochroną danych osobowych,
d) realizację zasad zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, prawidłowości, ograniczania przechowywania, integralności, poufności oraz rozliczalności przetwarzania danych osobowych.

§ 3. Sformułowanie strategii ochrony danych osobowych

Bezpieczeństwo Administratora to stan określony przez przyjęty zbiór norm, zasad, rozwiązań oraz środków i metod ochrony zasobów informacyjnych, którego miarą jest poziom ryzyka naruszenia dostępności, poufności lub integralności tych zasobów. Bezpieczeństwo Administratora jest zapewnione, jeżeli ryzyko naruszenia dostępności, poufności lub integralności chronionych zasobów Administratora nie przekracza akceptowalnych parametrów przy zachowaniu zasad sformułowanych w niniejszej Polityce Bezpieczeństwa Informacji i związanych z nią dokumentach.

§ 4. Regulacje ogólne

Ochronie podlegają w szczególności:

a) dane osobowe przetwarzane przez Administratora, niezależnie od ich formy i nośnika,
b) sprzęt wykorzystywany do przetwarzania, przesyłania i przechowywania danych osobowych u Administratora,
c) pomieszczenia, w których znajduje się kluczowy sprzęt informatyczny zawierający dane osobowe,

d) dokumenty i inne trwałe nośniki zawierające dane osobowe,
e) oprogramowanie wykorzystywane u Administratora,
f) pozostałe mienie wykorzystywane przez Administratora lub będące jego własnością,
g) informacje, których właścicielem są kontrahenci lub jednostki zewnętrzne współpracujące z Administratorem – w ramach tej współpracy.

§ 5. Uwarunkowania prawne

Niniejsza Polityka Bezpieczeństwa Informacji jest zgodna z przepisami obowiązującego prawa, w szczególności z:

- rozporządzeniem Parlamentu Europejskiego i Rady (UE) 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),
- ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych,
- ustawą z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (t.j. Dz. U. 2017 r. poz. 1219 z późn. zm.), jeżeli w danym przypadku przetwarzania ma zastosowanie,
- ustawą z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (t.j. Dz.U. 2017 poz. 1907 z późn. zm.), jeżeli w danym przypadku przetwarzania ma zastosowanie.

§ 6. Potencjalne zagrożenia

Zasoby Administratora, w szczególności informacje i dane osobowe, a także sprzęt niezbędny do ich przechowywania i przetwarzania, są istotne dla prowadzenia przez Administratora działalności gospodarczej. W szczególności identyfikuje się następujące kategorie zagrożeń, którym mogą podlegać zasoby Administratora:

a) naruszenie poufności danych zarówno przez pracowników, jak i osoby niezatrudnione u Administratora, w tym również przez kradzież zasobu,
b) niedostępność zasobu lub znaczna degradacja jego istotnych parametrów funkcjonalnych lub utrata danych (zniszczenie zasobu) na skutek wystąpienia sił wyższych albo nieumyślnego, umyślnego lub przypadkowego działania,
c) naruszenie integralności danych na skutek nieumyślnego, umyślnego lub przypadkowego działania,
d) stosowanie niespójnych zasad (standardów, procedur) i środków ochrony systemów.

2)Organizacja bezpieczeństwa informacji u Administratora

§7. Wykaz kategorii osób, których dane dotyczą oraz systemy informatyczne stosowane do przetwarzania tych danych

1) Administrator przetwarza dane osobowe w następujących zbiorach (bazach danych):
   a) Kandydaci na klientów i kontrahentów administratora, Klienci i Kontrahenci administratora;
   b) Pracownicy i inne osoby zatrudnione przez Administratora, byli pracownicy oraz kandydaci na pracowników i zatrudnionych przez Administratora.
2) Kategorie przetwarzanych danych osobowych (pola informacyjne):
   a) Imiona i nazwiska,
   b) Adresy zamieszkania lub pobytu bądź siedziba,
   c) Numery z istniejących rejestrów i ewidencji,
   d) Adresy poczty elektronicznej,
   e) Numery telefonów,
   f) Adresy stron internetowych,
   g) Daty, miejsca, ceny i zakresy dostarczonych osobie, której dane dotyczą produktów i usług przez administratora lub produktów i usług, którymi zainteresowana była osoba, której dane dotyczą,
   h) Zawód lub zajęcie oraz wykształcenie i uprawnieniach osoby, której dane dotyczą,

i) Dane o wcześniejszym zatrudnieniu oraz doświadczeniu i wiedzy,
j) Dane o uprawnieniach emerytalnych, rentowych,
k) Wizerunek w formie zdjęcia lub zapisu urządzenia rejestrującego obraz,
l) Informacje o niepełnosprawności.

3) Dane osobowe są przetwarzane w następujących systemach informatycznych i aplikacjach:
- system ERP Optima,
- system ERP XL,
- system Obiegu Dokumentów,
- program Płatnik (ZUS),
- program SYMFONIA,
- MOZILLA THUNDERBIRD,
- MS EXELL,
- MS WORD,
- MS POWERPOINT.

§ 8. Ewidencja osób upoważnionych

1) Administrator może prowadzić na trwałym nośniku „Ewidencję osób upoważnionych do przetwarzania danych osobowych", która składa się z następujących elementów:
a) imienia i nazwiska osoby upoważnionej
b) daty nadania upoważnienia
c) daty ustania upoważnienia
d) zakresu upoważnienia
e) identyfikatora osoby upoważnionej (dla danych przetwarzanych w systemie informatycznym)
f) podpisu osoby upoważnionej
g) podpisu osoby dokonującej wpisu w Ewidencji
2) Ewidencja jest aktualizowana i uzupełniana na bieżąco i niezwłocznie, a wpis nowej osoby do ewidencji następuje tylko po spełnieniu warunków, o których mowa w §15ust. 3.

§ 9. Poziomy bezpieczeństwa

1) Uwzględniając kategorie przetwarzanych danych oraz zagrożenia, a szczególnie fakt, że urządzenia systemu informatycznego są połączone z siecią publiczną wprowadza, się jednolity wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

§ 10. Przetwarzanie danych w systemie informatycznym

1) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie:
a) daty pierwszego wprowadzenia danych do systemu;
b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
d) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
2) Odnotowanie informacji, o których mowa w ust. 1 lit. a) i b), następuje automatycznie po zatwierdzeniu przez użytkownika operacji na danych.
3) Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system umożliwia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4) W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 11. Środki bezpieczeństwa

1) Środki bezpieczeństwa stosowane przez Administratora z uwzględnieniem wysokiego poziomu:
   A. Budynki, pomieszczenia lub części pomieszczeń, w których przetwarza się dane osobowe:
      a) budynki, pomieszczenia lub części pomieszczeń, w których przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych;
      b) przebywanie osób nieuprawnionych w obszarze, o którym mowa powyżej, jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych osobowych;
   B. System informatyczny:
      a) w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych;
      b) jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
         - w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
         - dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
      c) system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
         - działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
         - utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
      d) System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
      e) W przypadku zastosowania logicznych zabezpieczeń, o których mowa powyżej, obejmują one:
         - kontrolę przepływu informacji pomiędzy systemem informatycznym Administratora danych a siecią publiczną;
         - kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego Administratora danych.
      f) Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
   C. Identyfikator użytkownika, kopie zapasowe:
      a) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie;
      b) w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż, co 30 dni. Hasło składa się, co najmniej z 8 znaków w tym litery duże i małe oraz znak specjalny;
      c) kopie zapasowe:
         - przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
         - usuwa się niezwłocznie po ustaniu ich użyteczności.
   D. Transport urządzeń, na którym zapisane są dane osobowe:
      a) osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza budynkami, pomieszczeniami i częściami pomieszczeń, w których przetwarza się dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

E. Sposób postępowania z urządzeniami, dyskami lub innymi elektronicznymi nośnikami informacji, na których zapisane są dane osobowe:
   a) urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
      - likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
      - przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
      - naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora danych.
   b) Urządzenia i nośniki zawierające dane osobowe wrażliwe, przekazywane poza obszar, budynki, pomieszczenia i części pomieszczeń, w których przetwarza się dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

3) Inspektor Ochrony Danych Osobowych

§ 12. Powołanie Inspektora Ochrony Danych

Zgodnie z oceną przeprowadzona przez Administratora powołanie Inspektora Ochrony Danych Osobowych nie jest wymagane. Inspektor taki zostanie powołany przez Administratora w razie zajścia okoliczności uzasadniających jego powołanie.

§ 13. Zgłaszanie naruszeń ochrony danych osobowych

1) Administrator jest zobowiązany bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłosić je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2) Administrator dokumentuje na trwałym nośniku wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego przepisu.

§14. Ocena skutków przetwarzania dla ochrony danych osobowych i konsultacje

1) Jeżeli dany rodzaj przetwarzania danych osobowych przez Administratora – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przeprowadza ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2) Administrator przygotowuje dokument oceny, o której mowa w ust. 1 na trwałym. Dokument ten zawiera co najmniej:

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

3) Jeżeli ocena skutków dla ochrony danych, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym w trybie art. 36 rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

4) Obowiązki pracowników oraz kontrahentów i jednostek zewnętrznych

§ 15. Obowiązki pracowników

1) Niniejsza Polityka Bezpieczeństwa Informacji obowiązuje wszystkich pracowników Administratora, a każda osoba podejmująca pracę u Administratora lub inna osoba jeżeli uzyskują dostęp do danych osobowych, przyjmuje na siebie obowiązek zachowania w tajemnicy danych osobowych, z którymi ma styczność oraz sposobów ich zabezpieczenia.
2) Każdy zatrudniony pracownik, który uzyskuje dostęp do danych osobowych, w pierwszym dniu pracy ma obowiązek:
   a) zapoznać się z zasadami, regułami i postanowieniami niniejszej Polityki Bezpieczeństwa Informacji i potwierdzić ten fakt podpisując oświadczenie, które określa Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa Informacji,
   b) odbyć szkolenie z zakresu bezpieczeństwa informacji w tym ochrony danych osobowych, które potwierdzane jest w karcie szkolenia z zakresu bezpieczeństwa informacji lub w oświadczeniu pracownika.
3) Dostęp do danych osobowych pracownik otrzymuje dopiero po wydaniu mu pisemnego upoważnienia do przetwarzania danych osobowych oraz po podpisaniu oświadczenia, które stanowią załącznik nr 1, do niniejszej Polityki Bezpieczeństwa Informacji oraz po wpisie pracownika do Ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w §8, jeżeli jest prowadzona.
4) Pracownicy Administratora mają prawo używać danych osobowych, które przetwarza Administrator wyłącznie do celów służbowych, chyba, że regulacje szczegółowe stanowią inaczej.

§ 16. Obowiązki kontrahentów i jednostek zewnętrznych

1) Niniejsza Polityka Bezpieczeństwa Informacji obowiązuje wszystkich kontrahentów, jednostki zewnętrzne i ich pracowników, o ile w trakcie realizacji umowy otrzymują dostęp do zasobów informacyjnych Administratora.
2) W przypadku, gdy kontrahent w trakcie wykonywania umowy ma lub może mieć dostęp do zasobów informacyjnych Administratora, w umowach z kontrahentami wprowadzana jest klauzula dotycząca obowiązku przestrzegania bezpieczeństwa informacji. Klauzula ta powinna zawierać: zobowiązanie kontrahenta do przestrzegania Polityki Bezpieczeństwa Informacji,

ochrony udostępnionych zasobów informacyjnych poprzez ograniczenie ich kopiowania i udostępniania oraz do ich zwrotu lub zniszczenia w momencie zakończenia umowy.

3) Istotne naruszenie bezpieczeństwa informacji przez kontrahenta stanowi podstawę do odstąpienia przez Administratora od umowy i żądania pokrycia ewentualnej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.

§ 17. Wybór procesora lub podmiotu przetwarzającego

Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi wynikające z przepisów prawa i chroniło prawa osób, których dane dotyczą.

§ 18. Niezbędne elementy umowy

Z każdej umowy o przetwarzanie danych osobowych, umowy z procesorami lub podmiotami przetwarzającymi zawartej przez Administratora musi jednoznacznie wynikać, że podmiot przetwarzający:

1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3) podejmuje wszelkie środki bezpieczeństwa wymagane przepisami prawa;
4) korzysta on wyłącznie z usług innych podmiotów przetwarzających, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa i chroniło prawa osób, których dane dotyczą i jednocześnie nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody, a w przypadku ogólnej pisemnej zgody inny podmiot przetwarzający informuje podmiot przetwarzający o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym podmiotowi przetwarzającemu możliwość wyrażenia sprzeciwu wobec takich zmian;
5) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą;
6) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków wynikających z bezpieczeństwa przetwarzania, obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu oraz obowiązku zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;
7) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie;
8) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych umowie oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i

przyczynia się do nich, a w związku z tym obowiązkiem podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie przepisów prawa o ochronie danych.

Załącznik do Polityki Bezpieczeństwa Informacji:

1) Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem pracownika.

_____ [podpis organu reprezentacji Administratora]

Dokument przyjęty w dniu 25.05.2018