Polityka ochrony danych osobowych

KKSeals sp. z o. o. z siedzibą w Wolbromiu

przy ul. Ordona 5, 32-340 Wolbrom (dalej: „KKSeals")

1. Cel polityki ochrony danych osobowych

Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. 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),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.).

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. Definicje

2.1. **Administrator –** oznacza KKSeals sp. z o.o. z siedzibą w Wolbromiu, ul. Ordona 5, 32-340 Wolbrom,

2.2. **Dane osobowe –** wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można zidentyfikować na podstawie jednego bądź kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość, w tym – jeżeli dane te pozwalają na identyfikację

Użytkownika – IP urządzenia, dane o lokalizacji, identyfikator internetowy, czy informacje gromadzone za pośrednictwem plików cookies i innych podobnych technologii,

2.3. **RODO –** Rozporządzenie 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),

2.4. **Polityka –** niniejsza Polityka ochrony danych osobowych,

2.5. **Podmiot przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,

2.6. **Przetwarzanie –** operacja lub zestaw operacji wykonywanych lub danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

2.7. **Ustawa –** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.)

2.8. **Inspektor –** inspektor ochrony danych osobowych powołany przez Administratora

2.9. **Europejski Obszar Gospodarczy, EOG** – strefa wolnego handlu i wspólny rynek, obejmująca państwa Unii Europejskiej i Europejskiego Stowarzyszenia Wolnego Handlu (ang. EFTA), z wyjątkiem Szwajcarii.

2.10. **Organ nadzorczy –** niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,

2.11. **Unia –** Unia Europejska

3. Osoby odpowiedzialne za ochronę danych osobowych

3.1. Struktura organizacji ochrony danych osobowych:

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora, odpowiadają:

3.1.1. Administrator,

3.1.2. Inspektor Ochrony Danych,

3.1.3. Osoby upoważnione do przetwarzania danych osobowych.

3.2. Administrator wyznacza:

3.2.1. Inspektora ochrony danych osobowych,

3.3. Administrator jest odpowiedzialny za:

3.3.1. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,

3.3.2. wdrożenie odpowiednich procedur ochrony danych osobowych,

3.3.3. jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora ciążących na nim obowiązków,

3.3.4. zapewnienie środków umożliwiających prawidłowa realizację praw osób, których dane dotyczą,

3.3.5. prowadzenie rejestru czynności przetwarzania danych osobowych,

3.3.6. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,

3.3.7. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,

3.3.8. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,

3.3.9. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,

3.3.10. dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,

3.3.11. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,

3.3.12. nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

3.3.13. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,

3.3.14. w stosunku do Inspektora:

3.3.14.1. zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,

3.3.14.2. wspieranie Inspektora w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,

3.3.14.3. zagwarantowanie by Inspektor nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,

3.3.14.4. publikację danych kontaktowych Inspektora oraz zawiadomienie o nich organu nadzorczego.

3.4. Administrator nadzoruje działania Inspektora oraz wydaje mu zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.

3.5. Administrator każdorazowo wyraża zgodę na ostateczną akceptację na kluczowe z perspektywy organizacji działania Inspektora, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

3.6. Funkcję Inspektora pełni osoba wyznaczona przez Administratora.

3.7. Inspektor jest wyznaczany przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.

3.8. Do zadań Inspektora należy:

3.8.1. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,

3.8.2. monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,

3.8.3. monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,

3.8.4. doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora),

3.8.5. działania zwiększające świadomość pracowników Administratora w zakresie obowiązków wynikających z RODO lub przyjętych procedur,

3.8.6. szkolenia dla pracowników Administratora uczestniczących w operacjach przetwarzania danych,

3.8.7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,

3.8.8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,

3.8.9. współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,

3.8.10. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

3.9. Osoby upoważnione do przetwarzania danych osobowych

3.9.1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.

3.9.2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3.9.3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.

4. Ogólne zasady przetwarzania danych osobowych

4.1. Przetwarzanie danych osobowych w strukturze Administratora odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:

4.1.1. zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (zasada legalności),

4.1.2. w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (zasada rzetelności),

4.1.3. w sposób przejrzysty dla osób, których dane dotyczą (zasada przejrzystości),

4.1.4. w konkretnych, wyraźnych i prawnie uzasadnionych celach (zasada ograniczenia celu),

4.1.5. w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (zasada minimalizacji danych),

4.1.6. przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (zasada prawidłowości),

4.1.7. przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (zasada ograniczenia przechowywania),

4.1.8. w sposób zapewniający odpowiednie bezpieczeństwo (integralność i poufność).

4.2. Administrator gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

5. Zakres przetwarzania danych osobowych

5.1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.

5.2. Administrator prowadzi:

5.2.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,

5.2.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.

5.3. Rejestr, o którym mowa w pkt 6.2.1. zawiera co najmniej następujące informacje:

5.3.1. nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów,

5.3.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,

5.3.3. imię i nazwisko oraz dane kontaktowe Inspektora,

5.3.4. cele przetwarzania,

5.3.5. opis kategorii osób, których dane dotyczą,

5.3.6. opis kategorii danych osobowych,

5.3.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

5.3.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

5.3.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

5.3.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

5.4. Rejestr, o którym mowa w pkt 6.2.2. zawiera co najmniej następujące informacje:

5.4.1. nazwę oraz dane kontaktowe Administratora,

5.4.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator,

5.4.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator,

5.4.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe Inspektora każdego administratora, w imieniu którego działa Administrator,

5.4.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

5.4.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

5.4.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

5.5. Administrator prowadzi rejestry, o których mowa w pkt 6.2. w formie elektronicznej.

5.6. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator udostępnia mu prowadzone przez siebie rejestry.

6. Dopuszczenie osób do przetwarzania danych osobowych

6.1. Administrator realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.

6.2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora.

6.3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.

6.4. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

7. Powierzenie przetwarzania danych osobowych

7.1. Administrator realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.

7.2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.

7.3. Zawierana przez Administratora umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:

7.3.1.przedmiot powierzenia,

7.3.2.czas trwania powierzenia,

7.3.3.charakter i cel przetwarzania,

7.3.4.rodzaj powierzanych danych osobowych,

7.3.5.kategorie osób, których dane dotyczą,

7.3.6.warunki podpowierzenia przetwarzania danych

7.3.7.obowiązki i prawa Administratora,

7.3.8. obowiązki podmiotu przetwarzającego.

7.4. Umowa powierzenia może zostać zawarta zarówno w formie pisemnej, jak i elektronicznej.

7.5. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiada Administrator.

7.6. Administrator w terminie 7 dni przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym Inspektora oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez Inspektora.

7.7. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora lub udzielonymi pełnomocnictwami.

7.8. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.

7.9. Administrator ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.

7.10. Administrator w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

8. Udostępnienie danych osobowych

8.1. Administrator realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.

8.2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.

8.3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

9. Przekazywanie danych osobowych do państw trzecich

9.1. Przekazywanie danych, których administratorem jest Administrator do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.

9.2. Przekazanie danych osobowych, których administratorem jest Administrator do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

9.3. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 10.2, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy Administrator samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia Administrator może zapewnić za pomocą:

9.3.1. prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,

9.3.2. wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,

9.3.3. standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,

9.3.4. standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,

9.3.5. zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub

9.3.6. zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

9.4. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w pkt 10.3. Administrator może zapewnić w szczególności za pomocą:

9.4.1. klauzul umownych między Administratorem lub podmiotem przetwarzającym a Administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub

9.4.2. postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

9.5. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 10.2. oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 10.3. i 10.4. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:

9.5.1. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,

9.5.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,

9.5.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,

9.5.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

9.5.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,

9.5.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub

9.5.7. przekazanie nastąpi z publicznego rejestru.

10. Współadministrowanie danymi osobowymi

10.1. Administrator w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.

10.2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator oraz co najmniej jeden inny podmiot muszą:

10.2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,

10.2.2. muszą wspólnie ustalić cele przetwarzania danych,

10.2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.

10.3. W przypadku spełnienia warunków, o których mowa w pkt 11.2. Administrator oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.

10.4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

10.5. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora procesów przetwarzania danych osobowych pojawią się procesy wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, Administrator informuje o tym fakcie Inspektora.

10.6. Inspektor dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.

10.7. W przypadku, kiedy wynik oceny, o której mowa w pkt 11.6 wskazuje na współadministrowanie danymi osobowymi, Inspektor, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 11.4.

11. Realizacja praw osób, których dane dotyczą

11.1. Administrator uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:

11.1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),

11.1.2. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),

11.1.3. prawo do sprostowania danych (art. 16 RODO),

11.1.4. prawo do usunięcia danych (prawo do bycia zapomnianym) (art. 17 RODO),

11.1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),

11.1.6. prawo do przenoszenia danych (art. 20 RODO),

11.1.7. prawo sprzeciwu (art. 21 RODO),

11.1.8. prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

12. Ocena skutków dla ochrony danych osobowych

12.1. Administrator dokonuje oceny skutków dla ochrony danych w celu opisania przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.

12.2. W strukturze Administratora ocena skutków dla ochrony danych osobowych stanowi narzędzie rozliczalności ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.

13. Incydenty ochrony danych osobowych

13.1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, jest: Administrator oraz Inspektor.

14. Ogólne zasady bezpieczeństwa ochrony danych osobowych

14.1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.

14.2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

14.3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.

14.4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.

14.5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

14.6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.

14.7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji kopia ukryta.

14.8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.

14.9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. czystego biurka, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.

14.10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

14.11. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.

14.12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.

14.13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.

14.14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

14.15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.

14.16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.

14.17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.

14.18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

15. Przeglądy i aktualizacja polityki ochrony danych osobowych

15.1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.

15.2. Przeglądu Polityki dokonuje Administrator.

15.3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:

15.3.1. procesów funkcjonujących w strukturach Administratora,

15.3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator.

15.4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora przegląd Polityki wykonywany jest niezwłocznie.

15.5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Administrator dokonuje aktualizacji Polityki w wymaganym zakresie.

Zarząd KKSeals Sp. z o.o.