POLITYKA BEZPIECZEŃSTWA
w zakresie przetwarzania i ochrony danych osobowych
w spółce Think Kong sp. z o.o. z siedzibą w Warszawie
przyjęta dla potrzeb akcji pod hasłem „Paczki Wdzięczności"

§ 1
Postanowienia ogólne

1. Niniejszy dokument (dalej jako „Polityka Bezpieczeństwa") opisuje sposób zapewnienia bezpieczeństwa danych osobowych, które zostaną zgromadzone przez Spółkę w związku z przeprowadzeniem akcji pod hasłem „Paczki Wdzięczności" (dalej jako „Akcja") oraz wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.
2. Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych, przetwarzanych w ramach Akcji, rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
3. Administratorem danych, o których mowa w ust. 1 powyżej, jest Think Kong sp. z o.o. z siedzibą w Warszawie, przy ul. Wolskiej 88, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000333041, której akta rejestrowe przechowywane są w Sądzie Rejonowym dla m. st. Warszawy w Warszawie, XII Wydziale Gospodarczym Krajowego Rejestru Sądowego, posiadająca numer NIP 527-26-06-512 (dalej jako „Spółka").
4. Polityka Bezpieczeństwa ma zastosowanie do wszystkich osób, którym zostaną ujawnione dane osobowe, zgromadzone w związku z przeprowadzeniem Akcji.
5. Polityka Bezpieczeństwa jest zgodna z obowiązującymi przepisami prawa, w szczególności z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) (dalej jako „Ustawa") oraz wydanymi na jej podstawie aktami wykonawczymi.
6. Utrzymanie bezpieczeństwa danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot Polityki Bezpieczeństwa. Użyte wyżej pojęcia związane z zapewnieniem bezpieczeństwa oznaczają:
    a. poufność informacji – właściwość polegająca na tym, że dane osobowe nie będą ujawniane ani udostępniane nieuprawnionym do ich przetwarzania osobom ani podmiotom,
    b. integralność informacji – właściwość polegającą na zapewnieniu dokładności i kompletności informacji a także zapewnieniu, że dane osobowe nie zostaną zmienione lub zniszczone w nieuprawniony sposób,

c. dostępność informacji – właściwość polegającą na tym, że osoby upoważnione do przetwarzania danych osobowych mają dostęp do informacji i związanych z nią zasobów, w czasie w którym dostęp taki jest im potrzebny.

§ 2
Definicje

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, które zostały wskazane przez Uczestników Akcji w formularzu na Stronie Akcji,
2. przetwarzanie danych osobowych - gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
3. Strona Akcji – www.paczkiwdziecznosci.pl,
4. użytkownik - osoba upoważniona do przetwarzania danych osobowych, wskazanych przez Uczestników Akcji,
5. administrator systemu informatycznego - osoba upoważniona do zarządzania systemem informatycznym,
6. system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
7. Ustawa – ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
8. zabezpieczenie systemu informatycznego - wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą,
9. Uczestnicy Akcji – osoby, które w czasie trwania Akcji wypełnią, znajdujący się na Stronie Akcji, formularz i wskażą osobę lub organizację, od której oni lub inna osoba w latach 80-tych XX wieku otrzymali paczkę z pomocą lub opiszą w jaki sposób paczka ta pomogła osobie obdarowanej.

§ 3
Zakres zastosowania Polityki Bezpieczeństwa

1. Zakres przedmiotowy Polityki Bezpieczeństwa obejmuje:
   a. dane osobowe Uczestników Akcji oraz osób przez nich wskazanych,
   b. informacje dotyczące sposobu zabezpieczenia danych osobowych w szczególności nazwy kont i haseł w systemach przetwarzania danych osobowych,
   c. listy osób uprawnionych do przetwarzania danych osobowych.

2. Zakres podmiotowy Polityki Bezpieczeństwa obejmuje wszystkie osoby świadczące pracę na rzecz Spółki, zarówno na podstawie stosunku pracy jak i stosunku cywilnoprawnego, które zostały upoważnione do przetwarzania danych osobowych.
3. Polityka Bezpieczeństwa ma także zastosowanie do systemów informatycznych Spółki, w których przetwarzane są dane osobowe, a w szczególności do:
   a. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, w których przetwarzane są dane osobowe podlegające ochronie,
   b. wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

§ 4
Dostęp do informacji

1. Do przetwarzania danych osobowych może zostać dopuszczona tylko ta osoba, która została upoważniona przez Spółkę do ich przetwarzania.
2. Upoważnienie, o którym mowa w ust. 1 powyżej, powinno zawierać zakres działań przy przetwarzaniu danych, do którego dana osoba będzie upoważniona.
3. Upoważnienie, o którym mowa w ust. 1 powyżej, zostanie udzielone jedynie tym osobom, które muszą mieć dostęp do danych osobowych, aby móc zrealizować cel Akcji.
4. Każda osoba upoważniona do przetwarzania danych osobowych musi zostać wpisana na listę osób upoważnionych. Lista, o której mowa w zdaniu poprzednim, prowadzona jest przez Administratora Bezpieczeństwa Informacji.
5. Każda osoba, której zostanie udzielony dostęp do danych osobowych zobowiązana jest, przed przystąpieniem do ich przetwarzania, odbyć szkolenie dotyczące obowiązujących w zakresie ochrony danych osobowych przepisów prawa oraz zasad ochrony danych osobowych, wynikających z niniejszej Polityki Bezpieczeństwa.
6. Zakres zadań powierzonych osobie, dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę powierzonych jej danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.
7. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

§ 5
Zarządzanie danymi osobowymi

1. Za bezpieczeństwo danych osobowych w Spółce odpowiada Administrator Bezpieczeństwa Informacji.
2. Spółka, jako administrator danych osobowych, wyznacza do pełnienia funkcji Administratora Bezpieczeństwa Informacji Marka Roj (dalej jako „Administrator Bezpieczeństwa Informacji").

3. Spółka może w każdym czasie odwołać upoważnienie do przetwarzania danych osobowych udzielone Administratorowi Bezpieczeństwa Informacji albo innej osobie, której powierzyła ich przetwarzanie.
4. Do obowiązków Administratora Bezpieczeństwa Informacji, należy przede wszystkim nadzorowanie przestrzegania zasad ochrony danych osobowych.
5. Do obowiązków Administratora Bezpieczeństwa Informacji należy również:
    a. określenie wymagań bezpieczeństwa przetwarzania danych osobowych,
    b. nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych,
    c. określenie strategii zabezpieczania systemów informatycznych Spółki,
    d. określanie potrzeb w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
    e. prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych,
    f. zatwierdzanie wniosków w sprawie przyznania nowemu użytkownikowi identyfikatora oraz prawa dostępu do informacji chronionych w danym systemie informatycznym,
    g. prowadzenie ewidencji baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
    h. prowadzenie listy osób, którym zostało powierzone przetwarzanie danych osobowych,
    i. sprawowanie nadzoru nad obiegiem oraz sposobem przechowywania nośników, na których zostały zapisane dane osobowe,
    j. sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
    k. identyfikacja i analiza zagrożenia oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Spółki,
    l. analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia ochrony danych osobowych i przygotowanie oraz przedstawienie administratorowi danych zaleceń i rekomendacji dotyczących eliminacji ryzyk ich ponownego wystąpienia.

§ 6
Przetwarzanie danych osobowych

1. Dane osobowe mogą być przetwarzane z użyciem systemu informatycznego.
2. Dane osobowe mogą być przetwarzane w siedzibie Spółki, we wszystkich jej pomieszczeniach.

3. Systemy informatyczne, służące do przetwarzania danych osobowych, muszą być zgodne z wymogami, określonymi w obowiązujących aktach prawnych, regulujących zasady gromadzenia i przetwarzania danych osobowych.
4. Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów informatycznych.
5. Kopie bezpieczeństwa oraz dokumenty zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

§ 7
Sposób zabezpieczenia danych osobowych

1. Administrator danych osobowych ma obowiązek zastosować środki techniczne i organizacyjne, które zapewnią ochronę przetwarzanych danych osobowych w systemach informatycznych i na nośnikach tradycyjnych. Administrator danych osobowych ma obowiązek w szczególności zabezpieczyć dane osobowe przed:
   a. ich udostępnieniem osobom nieupoważnionym do ich przetwarzania,
   b. zmianą lub zabraniem przez osobę nieuprawnioną,
   c. przetwarzaniem z naruszeniem Ustawy oraz
   d. utratą, uszkodzeniem lub zniszczeniem.
2. Do zastosowanych środków technicznych należy:
   a. przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach,
   b. zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1 powyżej,
   c. wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji i nośników danych.
3. Do zastosowanych środków organizacyjnych należy:
   a. zapoznanie każdej osoby, upoważnionej do przetwarzania danych osobowych, przed jej przystąpieniem do pracy, z odpowiednimi przepisami dotyczącymi ochrony danych osobowych podczas ich przetwarzania,
   b. poinstruowanie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń
      i programów związanych z przetwarzaniem i ochroną danych osobowych,
   c. kontrolowanie otwierania i zamykania pomieszczeń, w których będą przetwarzane dane osobowe
4. Ochrona zbiorów danych osobowych polega na zabezpieczeniu informacji wprowadzonej, przetwarzanej, przesyłanej w systemie informatycznym oraz na nośnikach informacji przed nielegalnym ujawnieniem, kradzieżą lub nieuprawnioną modyfikacją czy usunięciem.
5. Mechanizmu wchodzące w skład systemów informatycznych należy wykorzystywać w celu ochrony danych przechowywanych w tych systemach informatycznych.

6. Dane osobowe mogą być przetwarzane jedynie przez osoby, którym udzielono upoważnienia do ich przetwarzania. Osoby upoważnione do przetwarzania danych mają obowiązek zachowania tajemnicy zarówno w odniesieniu do samych danych, które przetwarzają, jak i w odniesieniu do sposobów zabezpieczenia tych danych.
7. Osoby, którym nie udzielono upoważnienia do przetwarzania danych osobowych, nie mogą tych danych przetwarzać. Osoby te mogą przebywać w obszarach, w których dane osobowe są przetwarzane jedynie za uprzednią zgodą Administratora Bezpieczeństwa Informacji oraz jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych.
8. Przebywanie osób nieupoważnionych w obszarach przetwarzania danych osobowych jest monitorowane przez rejestrację tychże osób w książkach wejść i wyjść do poszczególnych obszarów lub pomieszczeń.
9. Wszystkie pomieszczenia, w których przetwarza się dane osobowe, powinny być zamykane na klucz po opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy.
10. Po zakończonej pracy klucze do pomieszczeń, w których przetwarzane są dane osobowe, powinny zostać oddane upoważnionemu pracownikowi obsługi gospodarczej, który zabezpieczy je, przed nieuprawnionym dostępem, w odpowiednio wyznaczonym do tego miejscu. Fakt przyjęcia kluczy przez pracownika Obsługi gospodarczej powinien zostać odnotowany w odpowiedniej ewidencji lub rejestrze.
11. Dane osobowe po zakończeniu ich przetwarzania, powinny zostać zniszczone w niszczarkach lub przekazane do zniszczenia specjalizującemu się w tym zakresie podmiotowi.
12. Osoby przetwarzające dane osobowe w systemach teleinformatycznych zobowiązane są stosować wygaszacze ekranu, indywidualne hasła lub kody dostępu do klawiatury oraz ustawiać monitory w taki sposób aby wyświetlana na nich informacja nie była widoczna dla osób nieuprawnionych.
13. Udostępnianie innym osobom indywidualnego kodu dostępu i haseł jest zabronione.
14. Zabronione jest również korzystanie, w systemach przetwarzających dane osobowe, z prywatnych nośników informacji.
15. Nie wolno korzystać z sieci publicznej (World Wide Webside) poprzez nieautoryzowane przeglądarki internetowe lub witryny internetowe nieznajomego pochodzenia (domeny zagraniczne tj. com itp.), jeżeli ich treść wskazuje na zwiększone ryzyko występowania oprogramowania szpiegowskiego, hakerskiego, spamowego, wirusowego.
16. W razie zgłoszenia żądania udostępniania danych użytkownicy zobowiązani są postępować zgodnie z przepisami Ustawy. Decyzję o udostępnieniu danych osobowych albo odmowie ich udostępnienia podejmuje Administrator Bezpieczeństwa Informacji.
17. Dla danych osobowych przetwarzanych w systemach informatycznych stosuje się następujące zasady:
    a. kontrola dostępu do zbiorów danych osobowych,

b. indywidualne identyfikatory użytkowników (pracowników przetwarzających dane osobowe),

c. uwierzytelnianie użytkowników (potwierdzanie ich tożsamości).

18. W celu zabezpieczenia danych osobowych, przetwarzanych w systemach informatycznych, przed ich utratą lub uszkodzeniem zastosowano następujące zabezpieczenia:

a. dla wszystkich systemów wdrożono procedury tworzenia kopii zapasowych;

b. wszystkie systemy informatyczne wyposażono w awaryjne zasilanie,

c. wdrożono oprogramowanie antywirusowe,

d. dostęp do systemów z sieci publicznej jest kontrolowany za pomocą zapory sieciowej oraz filtrów antyspamowych i oprogramowania antywirusowego,

e. poszczególne lokalizacje są połączone za pomocą sieci LAN,

f. przy przesyłaniu danych osobowych przez sieć publiczną użytkownicy są zobowiązani stosować oprogramowanie szyfrujące,

g. zastosowano środki fizyczne, chroniące urządzenia przed dostępem do nich przez osoby nieupoważnione do przetwarzania tych danych oraz przed zagrożeniami ze strony sił natury.

19. Użytkownicy, którzy korzystają z systemów przetwarzających dane osobowe za pomocą systemu teleinformatycznego, zobowiązani są do łącznego spełnienia poniższych warunków:

a. ustalenia hasła dostępu do systemu teleinformatycznego, które będzie zawierało nie mniej niż 8 (osiem) znaków, przy czym część z nich będzie pisana małą, a część wielką literą, ponadto hasło będzie zawierało cyfry lub znaki specjalne,

b. dokonywania zmiany ustalonego zgodnie z wytycznymi zawartymi w pkt a. powyżej hasła, nie rzadziej niż raz na 30 dni kalendarzowych,

c. ustalenia hasła, które wcześniej nie występowało.

20. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie Administratorowi Bezpieczeństwa Informacji, który niezwłocznie ustali nowe hasło.

21. Zabezpieczanie danych osobowych przed ich utratą uszkodzeniem, lub nieupoważnionym przetworzeniem w pozostałych przypadkach:

a. w przypadku naprawy, przekazania, likwidacji nośnika (m.in. dysk twardy, płyta kompaktowa, pamięć przenośna, dyskietka, taśma magnetyczna itp.), który zawiera dane osobowe podmiotowi nieupoważnionemu do przetwarzania danych, należy zapewnić trwałe wymazanie informacji stanowiących dane osobowe,

b. jeżeli użytkownik, korzystania z komputera przenośnego, który zawiera przetwarzane przez niego dane osobowe, to w czasie korzystania z tego urządzenia poza obszarem przetwarzania danych (siedzibą Spółki), powinien zachować szczególną ostrożność, m.in. mechanizmy szyfrowania plików lub baz danych wbudowanych w system operacyjny,

c. jeżeli ustanie konieczność przetwarzania danych osobowych na komputerze przenośnym, użytkownik powinien dane te usunąć z właściwego nośnika w sposób trwały, uniemożliwiający dostęp do nich osobom trzecim.

§ 8

Postępowanie w przypadku naruszenia ochrony przetwarzania danych osobowych

1. Każda osoba, przetwarzająca dane osobowe, zobowiązana jest do niezwłocznego poinformowania Administratora Bezpieczeństwa Informacji o każdym przypadku:
   a. naruszenia zabezpieczeń systemu informatycznego, za pomocą którego przetwarzane są dane osobowe,
   b. naruszenia stanu technicznego urządzeń, za pomocą których przetwarzane są dane osobowe,
   c. naruszenia zawartości zbioru danych osobowych,
   d. innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych.
2. Jeżeli nie jest możliwe niezwłoczne poinformowanie Administratora Bezpieczeństwa Informacji o zdarzeniach, o których mowa w pkt. 1 powyżej, należy niezwłocznie poinformować o nich bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce naruszenia danych osobowych Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, należy w szczególności:
   a. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość,
   b. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia
4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administratora Bezpieczeństwa Informacji lub upoważniona przez niego osoba w szczególności:
   a. zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji,
   b. może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   c. nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji
5. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. ABI dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:
   a) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych
      w związku z naruszeniem lub ujawnieniem ochrony danych osobowych,
   b) określenie czasu i miejsca: naruszenia lub ujawnienia danych osobowych i powiadomienia o tym fakcie,
   c) rodzaju naruszenia lub ujawnienia danych osobowych ,
   e) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
7. Raport, o którym mowa w ust. 6 powyżej Administrator Bezpieczeństwa Informacji przekazuje niezwłocznie administratorowi danych osobowych.

§ 9
Archiwizowanie informacji zawierających dane osobowe

Archiwizację dokumentów zawierających dane osobowe prowadzi się w odpowiednio zabezpieczonych pomieszczeniach i na właściwie zabezpieczonych nośnikach informatycznych lub tradycyjnych. Dane zbędne dla prowadzonych spraw są natychmiast niszczone poprzez działania fizyczne i informatyczne uniemożliwiające ich odczytanie.

§ 10
Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Bezpieczeństwa może być podstawą rozwiązania stosunku pracy lub umowy cywilnoprawnej bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Polityce Bezpieczeństwa mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.
3. Pracownicy Spółki zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa, w wypadku odrębnych od zawartych w niniejszym dokumencie uregulowań występujących w innych procedurach obowiązujących w Spółce, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
4. Polityka Bezpieczeństwa przechowywana jest przez Administratora Bezpieczeństwa Informacji.