POLITYKA BEZPIECZEŃSTWA
W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH
W FIRMIE AUTOBAGI POLSKA SP. Z O. O.

WPROWADZENIE

W celu zapewnienia ochrony przetwarzanych danych osobowych Administrator Danych Osobowych Autobagi Polska sp. z o.o. na podstawie art. 32 Rozporządzenia Parlamentu Europejskiego i Rady UE nr 2016/679 z dnia 27.4.2016 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 - RODO), wprowadza poniższą Politykę Bezpieczeństwa.

Rozdział I Definicje i postanowienia ogólne

§ 1 Zasady ochrony danych osobowych

1. Polityka Bezpieczeństwa reguluje sprawy ochrony zbiorów danych osobowych zarządzanych przez Administratora Danych Osobowych. Administrator Danych Osobowych, w trosce o bezpieczeństwo danych, wdrożył system zarządzania bezpieczeństwem danych osobowych, na zasadach określonych poniżej. Celem Polityki Bezpieczeństwa jest określenie kierunków działań dla zapewnienia bezpieczeństwa przetwarzania zbiorów danych osobowych zarządzanych przez Administratora Danych.
2. Polityka Bezpieczeństwa określa zasady ochrony danych osobowych osób fizycznych.
3. Przez bezpieczeństwo przetwarzania danych należy rozumieć:

a) Poufność - zapewnienie, że dane są dostępne jedynie osobom upoważnionym oraz nie są udostępniane osobom trzecim;
b) Integralność – zapewnienie dokładności i kompletności danych oraz metod przetwarzania;
c) Dostępność – zapewnienie, że osoby, których dane są przetwarzane mają dostęp do danych i związanych z nim aktywów wtedy, gdy tego zażądają;
d) Rozliczalność – zapewnienie, że działania danych osób można jednoznacznie przypisać tym osobom oraz bieżące rozliczanie operacji wykonywanych na informacjach poprzez zapewnienie przechowywania pełnej historii dostępu do danych;
e) Bieżące usuwanie danych z bazy w momencie, gdy ich przetwarzanie staje się zbędne.

§ 2 Zakres zbieranych danych osobowych

Niniejsza Polityka Bezpieczeństwa została opracowana, wdrożona i będzie utrzymywana w oparciu o obowiązujące przepisy RODO i obejmuje ona następujący zakres:

1) zbieranie danych osobowych dotyczących użytkowników Strony Internetowej www.kamazpolska.pl, oraz Sklepu Internetowego, którzy dokonali zakupów bez rejestracji lub założyli konto lub zgodzili się na przetwarzanie danych w celach marketingowych lub zgłosili chęć zapisania się do listy mailingowej celem otrzymywania newslettera,
2) Polityka Bezpieczeństwa stosowana jest we wszystkich oddziałach i placówkach Administratora Danych Osobowych,
3) Polityka Bezpieczeństwa dotyczy wszystkich pracowników Administratora Danych Osobowych w rozumieniu kodeksu pracy, a także współpracowników tj. osób współpracujących na podstawie umów cywilnoprawnych oraz stażystów i praktykantów, którzy mają lub będą mieć dostęp do informacji podlegających ochronie.
4) W zbiorach danych administrowanych przez Administratora Danych Osobowych zabrania się przetwarzania danych wrażliwych ujawniających:
   a) stan zdrowia
   b) pochodzenie rasowe lub etniczne
   c) poglądy polityczne
   d) przekonania religijne lub światopoglądowe
   e) przynależność wyznaniową
   f) przynależność partyjną i związkową
   g) dane genetyczne
   h) dane biometryczne
   i) nałogi
   j) orientację seksualną.

§ 3 Słownik

Przez użyte w treści Polityki Bezpieczeństwa sformułowania należy rozumieć:

a) Administrator Danych Osobowych – Autobagi Polska sp. z o. o. z siedzibą w Libertowie";
b) System informatyczny – zespół środków technicznych, technicznych skład którego wchodzą urządzenia: komputerowe, drukujące, łączności, wraz z okablowaniem i oprogramowaniem, zabezpieczeń także zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieci informatyczne i udostępniane przez nią zasoby;
c) Przetwarzanie danych – wszystkie czynności wykonywane na danych, w tym szczególnie gromadzenie, utrwalanie, modyfikacja, usuwanie, przechowywanie, przenoszenie i przekazywanie, niezależnie od formy, w jakiej wykonywane są te czynności;

d) Osoby zatrudnione przy przetwarzaniu danych osobowych – wszystkie osoby, w tym użytkownicy systemu teleinformatycznego, mające z racji wykonywanych obowiązków dostęp do danych osobowych.

Rozdział II Ochrona przetwarzania danych osobowych

§ 4 Administrator Bezpieczeństwa Danych

1. W ramach zapewnienia realizacji niniejszej Polityki ustanawia się Administratora Bezpieczeństwa Danych, który odpowiada za realizację niniejszej Polityki oraz zapewnienie bezpiecznego przechowywania danych zgodnie z niniejszą Polityką i przepisami prawa. Funkcje Administratora Bezpieczeństwa Danych pełni Wojciech Traczuk.
2. Administrator Bezpieczeństwa Danych prowadzi listę pracowników i współpracowników, którzy mają dostęp do chronionych danych, tzn. posiadają upoważnienie nadane przez Administratora.
3. Lista pracowników lub współpracowników, którzy mają dostęp do chronionych danych znajduje się w odrębnym dokumencie „Ewidencja Upoważnień" i aktualizowana jest na bieżąco.
4. W ramach nadawania uprawnień do danych należy stosować zasadę „minimalnych uprawnień", to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku.

§ 5 Ocena ryzyka

1. Zapewnienie bezpieczeństwa informacji realizowane jest poprzez zarządzanie ryzykiem, na które składa się:
   - klasyfikacja zasobów i ich wartości,
   - uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania oraz związanego z tym ryzyka naruszenia praw osób, których dane dotyczą
   - uwzględnienie stanu wiedzy technicznej, kosztów wdrażania
   - identyfikacja stopnia zagrożeń i ich następstw przy uwzględnieniu kryteriów skutków utraty informacji, miejsca występowania zagrożeń, ryzyka utraty lub zniszczenia informacji,
   - określenie i wdrożenie działań zabezpieczających zasoby.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 6 Cele przetwarzania

1. Administrator Danych Osobowych przetwarza dane osobowe w celu i w zakresie niezbędnym do wykonania umowy sprzedaży towarów w tym za pośrednictwem Strony Internetowej sklep.kamazpolska.pl oraz w celach marketingowych.
2. Administrator Danych Osobowych przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w celach marketingowych, jeżeli osoba, której przetwarzane dane dotyczą wyrazi na to zgodę.

§ 7 Osoby odpowiedzialne

1. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy lub współpracownicy, którym przyznane zostało uprawnienie do przetwarzania danych.
2. Administrator Bezpieczeństwa odpowiedzialny jest za zapewnienie zasobów niezbędnych dla funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń.

§ 8 Uwzględnianie ochrony danych w fazie projektowania

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator wdraża odpowiednie środki techniczne i organizacyjne zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania.

§ 9 Domyślna ochrona danych

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Rozdział III Gromadzenie i udostępnianie danych osobowych

§ 10 Źródła pozyskania danych osobowych

Dane osobowe przetwarzane przez Administratora Danych Osobowych mogą być uzyskiwane bezpośrednio od klientów.

§ 11 Zasada minimalizacji celu

Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą.

§ 12 Prawo dostępu do danych osobowych

Administrator Danych Osobowych realizując Politykę Bezpieczeństwa w zakresie ochrony danych osobowych zapewnia klientom, których dane dotyczą:

1) Prawo potwierdzenia, że przetwarzane są dane osobowe dotyczące danej osoby
2) Prawo dostępu do przetwarzanych danych osobowych oraz prawo do jednej bezpłatnej kopii przetwarzanych danych
3) Prawo do udzielania informacji o przetwarzanych danych osobowych
4) Prawo sprostowania oraz uzupełnienia danych osobowych
5) Prawo do żądania przeniesienia danych osobowych
6) Prawo do żądania ograniczenia przetwarzania danych osobowych
7) Prawo do wniesienia sprzeciwu wobec przetwarzania

- na zasadach określonych w przepisach RODO.

Rozdział IV Opis zagrożeń ochrony danych osobowych

§ 13 Przewidywane zagrożenia dla danych osobowych

Administrator Danych Osobowych będzie stale doskonalił i rozwijał organizacyjne, techniczne oraz informatyczne środki ochrony przetwarzanych danych osobowych tak, aby skutecznie zapobiegać zagrożeniom związanymi m. in. z:

a) infekcjami wirusów i koni trojańskich, które instalując się na komputerze mogą wykradać zasoby tego komputera,
b) dostępem do stron internetowych, na części których zainstalowane są skrypty pozwalające wykradać zasoby komputera,
c) ogólnie dostępnymi komunikatorami internetowymi, w których występują luki, przez które można uzyskać dostęp do komputera,
d) użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku,
e) spamem, posiadającym niekiedy programy pozwalające wykradać zasoby komputera,
f) możliwością niekontrolowanego kopiowania danych na dyski wymienne (np.: CD, pendrive, DVD),
g) możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane (oprogramowanie typu sniffer, które może być również instalowane przez wirusy),
h) lekceważeniem zasad ochrony danych polegających na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia (np.: bez wylogowania się lub bez zabezpieczenia wygaszacza ekranu hasłem),

i) brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy (osób nieuprawnionych do przetwarzania danych),
j) atakami z sieci uniemożliwiającymi przetwarzanie,
k) działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści,
l) kradzieżą sprzętu lub nośników z danymi,
m) przekazywaniem sprzętu z danymi do serwisu naprawy,
n) kradzieżami tożsamości umożliwiającymi podszywanie się pod inną osobę,
o) podszywaniem się przez osoby nieuprawnione pod witrynę internetową, która zbiera dane i innym zagrożeniom mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

Rozdział V Środki bezpieczeństwa

§ 14 Obowiązki osób upoważnionych do przetwarzania danych

1. Każdy pracownik lub współpracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak hasła dostępowe, klucze, inne mechanizmy umożliwiające dostęp do bazy danych.
2. Przez ochronę danych dostępowych rozumie się w szczególności:
   1) nieprzekazywanie dostępów do bazy danych innym osobom,
   2) nieprzechowywanie danych w miejscach publicznych,
   3) ochronę danych dostępowych przed kradzieżą przez osoby trzecie.
3. W przypadku rozwiązania umowy o pracę z pracownikiem lub umowy cywilnoprawnej ze współpracownikiem, dezaktywowane są wszelkie jego dostępy.
4. Zabrania się przenoszenia niezabezpieczonych danych poufnych poza teren Administratora Danych Osobowych. W szczególności zabrania się przenoszenia niezabezpieczonych danych na nośnikach elektronicznych (np.: pendrive, nośniki CD) poza teren Administratora Danych Osobowych.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych zostaną zobowiązane do zachowania ich w tajemnicy.

§ 15 Szkolenia

1. Osoby zatrudnione przy przetwarzaniu danych zostaną zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
2. Osoby zatrudnione przy przetwarzaniu danych osobowych zostaną przeszkolone w zakresie zabezpieczeń systemu informatycznego i innych zabezpieczeń danych.

3. Administrator na bieżąco informuje pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

§ 16 Środki bezpieczeństwa fizyczne

1. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
2. Dokumenty zawierające dane osobowe przechowywane są w zamykanych szafkach.
3. Wprowadzona zostaje zasada: czystego biurka, czystego kosza, czystej drukarki, czystej kserokopiarki.
4. Administrator zapewnia ochronę przeciwpożarową danych osobowych.

§ 17 Środki bezpieczeństwa techniczne i organizacyjne

1. Ustala się następujące zasady dostępu do danych:
   1) dostęp do chronionych danych realizowany jest na przeznaczonych do tego serwerach i dyskach,
   2) dostęp do danych jest odnotowywany,
   3) uzyskanie dostępu poprzez użycie komputera przenośnego musi być dodatkowo zabezpieczone,
   4) uzyskanie dostępu do danych poprzez firmową sieć Wi-Fi odbywa się z wykorzystaniem kanału szyfrowanego.

2.Stacje robocze powinny być zabezpieczone przed nieautoryzowanym dostępem osób trzecich, poprzez użycie minimalnych środków ochrony takich jak:
   1) instalacja na stacjach systemów oprogramowania ochronnego typu firewall oraz antywirus,
   2) wdrożenie systemu aktualizacji systemu operacyjnego oraz jego składników,
   3) wymaganie podania hasła przed uzyskaniem dostępu do stacji,
   4) kontrola czy niezablokowane stacje PC nie pozostają bez nadzoru,
   5) bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

3. Ustala się następujące zasady wykorzystywania haseł:
   1) hasła powinny być okresowo zmieniane,
   2) hasła nie mogą być przechowywane w formie otwartej (niezaszyfrowanej),
   3) hasła powinny składać się z minimum 8 znaków, w tym małe i wielkie litery cyfry i jeden znak specjalny, nie mogą przybierać prostych form.

3. Korzystanie z nowych lub zmienionych urządzeń służących do przetwarzania informacji powinno być zweryfikowane na zgodność z wymaganiami systemu bezpieczeństwa i zaakceptowane przez Administratora Danych Osobowych.

4. Dane osobowe powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT w szczególności poprzez:
   a) zabezpieczenie nośników z kopiami zapasowymi, które powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym,

b) okresowe testowanie kopii zapasowych pod względem rzeczywistej możliwości odtworzenia danych.

§ 18 Prowadzenie dokumentacji dotyczącej ochrony danych osobowych

Administrator Ochrony Danych prowadzi dokumentację w zakresie:

1) obecnie wykorzystywanych metod zabezpieczeń danych,
2) ewentualnych naruszeń bezpieczeństwa danych osobowych
3) udzielonych upoważnień
4) rejestru czynności przetwarzania
5) udzielonych zgód na przetwarzanie danych w celach marketingowych.

§ 19 Zgłaszanie naruszeń ochrony danych osobowych

Wszelkie podejrzenia naruszenia bezpieczeństwa danych należy zgłaszać w formie ustnej lub za pośrednictwem poczty elektronicznej do Administratora Danych Osobowych. Każdy incydent jest odnotowywany w stosownej bazie danych, Administrator Danych Osobowych podejmuje stosowne kroki zaradcze.

§ 20 Zasady niszczenia danych osobowych

1. Administrator Danych Osobowych sprawuje kontrolę i nadzór nad niszczeniem zbędnych danych osobowych i ich zbiorów.
2. Niszczenie zbiorów danych osobowych polega w szczególności na trwałym, fizycznym zniszczeniu danych osobowych i ich zbiorów wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przy stosowaniu powszechnie dostępnych metod.

Rozdział VI Przeglądy i aktualizacje wdrożonych środków bezpieczeństwa

§ 21 Coroczna aktualizacja

System bezpieczeństwa danych osobowych podlega przeglądowi pod kątem aktualności i stosowalności w odstępach rocznych.

§ 22 Szczególne przypadki aktualizacji

Polityka Bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:

a) likwidacji, utworzenia lub zmiany zawartości informacyjnej zbioru,
b) zmiany lokalizacji zbioru,

c) zmiany opiekuna zbioru,
d) zmiany przepisów prawa dotyczącego ochrony danych osobowych, wymagającej aktualizacji Polityki.