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. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 1997 r. Nr 133 poz. 883) w związku z §3 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wprowadza poniższą Politykę Bezpieczeństwa.

Rozdział I Definicje i postanowienia ogólne

§ 1

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. 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

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

1) zbieranie danych osobowych dotyczących użytkowników Strony Internetowej www.kamazpolska.pl, którzy 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.

§ 3

Przez użyte w treści Polityki Bezpieczeństwa sformułowania należy rozumieć:

a) Administrator Danych Osobowych – Autobagi Polska sp. z o. o. z siedzibą w Libertowie";
b) Ustawa - Ustawa o ochronie danych osobowych, tekst jednolity Dz U. z 2002 r. nr 101. oz. 926. z póź. zm.;
c) 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;
d) 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;
e) 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

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.
3. Lista pracowników lub współpracowników, którzy mają dostęp do chronionych danych znajduje się w odrębnym dokumencie 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

1. Administrator Danych Osobowych w celu do właściwej i skutecznej ochrony danych osobowych, deklaruje zamiar:

a) Podejmowania wszelkich działań niezbędnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych;
b) Stałego podnoszenia kwalifikacji osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa przetwarzania tych danych;
c) Traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonywania przez zatrudnione osoby;
d) Systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych;
e) Aktualizacji informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz inni zagrożeniami danych, płynącymi z funkcjonowania systemu informatycznego oraz sieci teleinformatycznych;
f) Ochrony danych osobowych przed udostępnianiem ich osobom nieuprawnionym, przetwarzaniem niezgodnym z ustawą oraz niepożądaną zmianą lub uszkodzeniem.

§ 6

Zapewnienie bezpieczeństwa informacji realizowane jest poprzez:

1) zarządzanie ryzykiem, na które składa się:
- klasyfikacja zasobów i ich wartości,
- 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) zarządzanie zmianami, na które składa się:
- analiza wpływu zmian na poziom bezpieczeństwa,
- zapewnienie pełnej koordynacji podczas wprowadzania zmian.

§ 7

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

§ 8

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.
3. 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.

§ 9

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.

§ 10

1. Dane osobowe powinny być chronione równolegle na wielu poziomach, w celu zapewnienia pełniejszej oraz skuteczniejszej ochrony.
2. Dane osobowe powinny być chronione przed dostępem osób niepowołanych, oraz uszkodzeniem.

§ 11

W zbiorach danych administrowanych przez Administratora Danych Osobowych zabrania się przetwarzania danych ujawniających:

a) stan zdrowia
b) pochodzenie rasowe
c) poglądy polityczne
d) przekonania religijne lub filozoficzne
e) przynależność wyznaniową

f) przynależność partyjną i związkową
g) kod genetyczny
h) nałogi
i) preferencje seksualne

Rozdział III Gromadzenie i udostępnianie danych osobowych

§ 12

Dane osobowe przetwarzane przez Administratora Danych Osobowych mogą być uzyskiwane:

a) bezpośrednio od użytkowników Strony Internetowej www.kamazpolska.pl.

§ 13

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.

§ 14

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.

§ 15

Administrator Danych Osobowych realizując Politykę Bezpieczeństwa w zakresie ochrony danych osobowych zapewnia dostęp do przetwarzanych danych osobowych osobom fizycznym będącym dysponentami tych danych na ich wniosek skierowany do Administratora Danych Osobowych. Dane osobowe dotyczące danej osoby dostępne są tylko dla tej osoby i ma ona możliwość ich weryfikacji i korekty. Korekty danych osobowych dokonuje Administrator Danych Osobowych na umotywowany wniosek osoby, której dane dotyczą.

§ 16

1. Zbiory danych udostępnia się na umotywowany wniosek uprawnionej osoby, chyba że odrębne przepisy prawa stanowią inaczej.
2. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, w wypadkach przewidzianych obowiązującymi przepisami.

Rozdział IV Opis zagrożeń ochrony danych osobowych

§ 17

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

§ 18

Administrator Danych Osobowych danych osobiście nadzoruje przestrzeganie zasad ochrony przetwarzanych danych osobowych.

§ 19

Administrator Danych Osobowych danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, o której mowa w art. 39 ust. 1 ustawy o ochronie danych osobowych.

§ 20

Osoby zatrudnione przy przetwarzaniu danych zostaną zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

§ 21

Osoby zatrudnione przy przetwarzaniu danych osobowych zostaną przeszkolone w zakresie zabezpieczeń systemu informatycznego.

§ 22

Osoby zatrudnione przy przetwarzaniu danych osobowych zostaną zobowiązane do zachowania ich w tajemnicy.

§ 23

Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.

§ 24

Dostęp do informacji przechowywanych i przetwarzanych przez Administratora Ochrony Danych jest poddany kontroli wynikającej z obowiązujących przepisów prawa powszechnego oraz dodatkowych wymagań bezpieczeństwa. Kontrola może polegać na:

1) wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi,
2) zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny,
3) bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

§ 25

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 chronionych 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.
4. 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

§ 26

Administrator Ochrony Danych prowadzi dokumentację w zakresie:

1) obecnie wykorzystywanych metod zabezpieczeń danych,
2) ewentualnych naruszeń bezpieczeństwa systemów IT,
3) dostępów do zbiorów danych / systemów udzielonych pracownikom lub współpracownikom.

§ 27

Poufne dane powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT w szczególności poprzez:

1) zabezpieczenie nośników z kopiami zapasowymi, które powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym,
2) okresowe testowanie kopii zapasowych pod względem rzeczywistej możliwości odtworzenia danych.

§ 28

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.

Rozdział VI Przeglądy i aktualizacje Polityki Bezpieczeństwa

§ 29

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

§ 30

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.

WYKAZ ZAŁĄCZNIKÓW

1. Załącznik A

Wykaz zbiorów danych osobowych oraz sposób przepływu danych między poszczególnymi systemami

2. Załącznik B

Opis struktury zbiorów danych osobowych przechowywanych w systemach informatycznych

3. Załącznik C

Wzór upoważnienia do przetwarzania danych osobowych

4. **Załącznik D**

Ewidencja osób upoważnionych do przetwarzania danych osobowych

5. **Załącznik E**

Wykaz miejsc, w których przetwarzane są dane osobowe