POLITYKA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

w spółce MANN sp. z o. o.

z siedzibą w Chorzowie

I. Definicje

Pod pojęciami użytymi w dokumencie rozumie się:

1. **Administrator danych** – spółka MANN sp. z o. o. z siedzibą w Chorzowie przy ul. Kurta Aldera 44, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000528390, NIP: 6452540904, REGON: 243673630, o kapitale zakładowym w kwocie 40.000 złotych, która samodzielnie ustala cele i sposoby przetwarzania danych osobowy;
2. **Administrator Systemu informatycznego (ASI)** – osoba wyznaczona przez Administratora danych odpowiedzialna za zarządzanie systemami informatycznymi oraz stosowanie środków technicznych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe;
3. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"), także osoby fizycznej prowadzącej działalność gospodarczą; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4. **Inspektor Ochrony Danych (IOD)** – osoba odpowiedzialna za przestrzeganie zasad przetwarzania danych osobowych, która może być wyznaczona przez Administratora danych na podstawie art. 37 RODO;
5. **Instrukcja Bezpieczeństwa Systemu informatycznego** – dokument opisujący warunki zarządzania systemami informatycznymi oraz stosowane środki techniczne zapewniające ochronę przetwarzanych danych osobowych, w tym w szczególności przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe;
6. **osoba upoważniona** – osoba, której udzielono pisemnego upoważnienia do przetwarzania danych osobowych w zakresie wskazanym w Upoważnieniu;
7. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny lub jednostka nieposiadająca osobowości prawnej, która przetwarza dane osobowe w imieniu i na zlecenie Administratora danych, na podstawie umowy o świadczenie usług;
8. **Polityka bezpieczeństwa** – niniejsza Polityka bezpieczeństwa i ochrony danych osobowych;
9. **przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na 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;
10. **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);

11. **Upoważnienie** – dokument wystawiony przez Administratora danych, z którego wynika umocowanie do wykonywania w jego imieniu czynności związanych z przetwarzaniem danych osobowych;
12. **zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

II. Cele i zakres Polityki bezpieczeństwa

Polityka bezpieczeństwa wraz z Instrukcją Zarządzania Systemem informatycznym oraz załącznikami opisują działania organizacyjne i techniczne a także procedury podejmowane przez Administratora danych, których celem jest osiągnięcie i utrzymanie akceptowalnego poziomu bezpieczeństwa przetwarzanych danych osobowych oraz podniesienie poziomu świadomości pracowników i współpracowników w zakresie ochrony tych danych/informacji. Polityka bezpieczeństwa stanowi jednocześnie politykę ochrony danych w rozumieniu art. 24 ust. 2 RODO.

Dla celów niniejszej Polityki bezpieczeństwa przyjmuje się, że wszelkie prawa i obowiązki opisane w dokumencie przypisane Administratorowi traktować należy odpowiednio jako prawa i obowiązki podmiotu przetwarzającego w sytuacjach kiedy wymagane jest to przez postanowienia RODO, chyba że niniejszy dokument stanowi inaczej.

Celem Polityki jest wskazanie działań, które należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki Administratora w zakresie zabezpieczenia danych osobowych. Między innymi w tym celu u Administratora przeprowadzony został audyt wdrożenia RODO. Zakres przedmiotowy Polityki bezpieczeństwa obejmuje wszystkie zbiory danych osobowych określone w Rejestrze czynności przetwarzania opracowanym zgodnie z art. 30 RODO. Rejestr czynności przetwarzania stanowi Załącznik nr 1 do niniejszej Polityki bezpieczeństwa i będzie na bieżąco monitorowany i uaktualniany przez Administratora danych. Rejestr składa się z dwóch części: część pierwsza dotyczy przetwarzania danych osobowych jako Administrator, część druga – przetwarzania danych osobowych na podstawie umów o powierzenie przetwarzania danych osobowych.

Polityka bezpieczeństwa ma status dokumentu przeznaczonego do użytku wewnętrznego i może być udostępniona osobom trzecim jedynie za zgodą Administratora danych. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Administratora danych oraz osoby świadczące usługi na rzecz Administratora danych na podstawie umów cywilnoprawnych. Administrator danych deklaruje wolę ochrony przetwarzanych danych osobowych, której celem jest zapewnienie bezpieczeństwa tych danych, a w szczególności dbanie o ich:

a. poufność,
b. integralność,
c. dostępność,
d. rozliczalność,
e. minimalizację

oraz dołoży wszelkich starań, aby powyższe zasady były nadrzędnymi dla jego pracowników oraz współpracowników. Polityka bezpieczeństwa stanowi uzupełnienie i wykonanie wytycznych w zakresie ochrony danych osobowych płynących z RODO.

Dane osobowe objęte Polityką bezpieczeństwa oraz sposoby ich zabezpieczeń objęte są tajemnicą nieograniczoną w czasie.

Do wyznaczonego celu Administrator dąży poprzez wdrożenie odpowiedniego systemu ochrony danych osobowych przed zagrożeniami wewnętrznymi i zewnętrznymi.

Polityka bezpieczeństwa realizuje przepisy rozporządzenia z dnia 27 kwietnia 2016 roku Parlamentu Europejskiego i Rady 2016/679 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) - Dziennik Urzędowy UE L 119 z dnia 4 maja 2016.

III. Administrator danych

Administrator realizuje zadania, do których zalicza się podejmowanie wszelkich działań mających na celu zapewnienie ochrony przetwarzanych danych osobowych na najwyższym poziomie, w szczególności poprzez:

- formułowanie i wdrażanie warunków technicznych i organizacyjnych służących ochronie danych osobowych;
- podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w tym wyznaczenie Administratora Systemu informatycznego odpowiedzialnego za nadzór nad systemami, w których przetwarza się dane osobowe;
- weryfikację przestrzegania zasad przetwarzania danych osobowych oraz poziomu ochrony danych osobowych.

IV. Inspektor Danych Osobowych

U Administratora nie powołuje się Inspektora Danych Osobowych ponieważ nie zostały spełnione przesłanki wskazane w art. 39 ust. 1 RODO. W czasie analizy ryzyka oraz wdrażania postanowień RODO ustalono, że:

1. Administrator nie jest organem lub podmiotem publicznym, o którym mowa w art. 39 ust. 1 lit. a RODO;
2. główna działalność Administratora nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
3. główna działalność Administratora nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Powyższych ustaleń dokonywano w oparciu o motywy RODO oraz wytyczne Grupy Roboczej art. 29. W przypadku, w którym działalność Administratora wypełniać będzie jedną z powyższych przesłanek, Administrator niezwłocznie podejmie działania mające na celu powołanie Inspektora Danych Osobowych i uposażenie go w środki umożliwiające pełnienie funkcji.

V. Zarządzanie bezpieczeństwem

1. Zarządzanie bezpieczeństwem systemów jest procesem ciągłym, realizowanym przy współpracy Administratora danych z ASI.

2. Osoby, które w ramach powierzonych im obowiązków przetwarzają dane osobowe – bez względu na łączący je z Administratorem stosunek prawny – zobowiązane są do:
   a. przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, Polityką bezpieczeństwa, Instrukcją Zarządzania Systemem informatycznym oraz załącznikami do ww. dokumentów,
   b. przetwarzania danych osobowych jedynie w oparciu o Upoważnienie w granicach w nim określonych, a w przypadkach przewidzianych przepisami prawa, umowę o powierzenie przetwarzania danych osobowych.
3. Administrator danych podejmuje wszelkie działania celem umożliwienia osobom przetwarzającym dane osobowe na podstawie Upoważnienia ich przetwarzanie zgodnie z prawem.
4. Osoby przetwarzające dane osobowe podlegają odpowiedzialności służbowej oraz cywilnej.
5. Szczegółowe procedury dotyczące przetwarzania danych osobowych przewidziane zostały w następujących dokumentach stanowiących załączniki do niniejszej Polityki bezpieczeństwa:
   a. Powierzenie przetwarzania danych osobowych – Instrukcja (Załącznik nr 2) wraz z:
      - Umową powierzenia przetwarzania danych osobowych – wzór (Załącznik nr 2a).
   b. Upoważnienie do przetwarzania danych osobowych – Instrukcja (Załącznik nr 3) wraz z:
      - wzorem upoważnienia do przetwarzania danych osobowych dla pracownika (Załącznik nr 3a),
      - wzorem upoważnienia do przetwarzania danych osobowych dla zleceniobiorcy (Załącznik nr 3b),
      - wzorem zobowiązania osoby upoważnionej (Załącznik nr 3c),
      - rejestrem udzielonych upoważnień (Załącznik nr 3d).

VI. Zarządzanie systemem informatycznym

Opracowując dokument służący określeniu sposobu zarządzania systemami informatycznymi wykorzystywanymi do przetwarzania danych osobowych, używanymi w związku z działalnością prowadzoną przez Administratora, u Administratora wprowadzono Instrukcję Zarządzania Systemem informatycznym obejmujący swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych. Dokument stanowi Załącznik nr 4 do niniejszej Polityki bezpieczeństwa.

VII. Obowiązek informacyjny

Administrator – celem sprostania obowiązkom informacyjnym – stosuje instrukcje stanowiące załączniki do Polityki bezpieczeństwa. Klauzule informacyjne w zależności od potrzeby i możliwości technicznych Administratora stanowią części składowe dokumentów regulujących stosunek Administratora z podmiotem, któremu klauzule winne być przedstawione, bądź podawane są do wiadomości w sposób zwyczajowo przyjęty u Administratora.

Obowiązek informacyjny szczegółowo uregulowany został w dokumencie pn. Procedura informowania – instrukcja (Załącznik nr 5) wraz z:

- Załącznik nr 5a - Klauzule informacyjne dla Klientów usług transportowych,

- Załącznik nr 5b - Klauzule informacyjne dla Kontrahentów Administratora,
- Załącznik nr 5c - Klauzule informacyjne dla rekrutowanych pracowników,
- Załącznik nr 5d - Klauzule informacyjne dla pracowników,
- Załącznik nr 5e - Klauzule informacyjne dla kierowców,
- Załącznik nr 5f - Klauzule informacyjne dla zleceniobiorców.

VIII. Rozpoznawanie wniosków osób, których dane są przetwarzane

Opis praw osób, których dane są przetwarzane przez Administratora zamieszczono w dokumencie pn. „Prawa osób, których dane są przetwarzane – instrukcja" stanowiącym załącznik nr 6a do niniejszej Polityki bezpieczeństwa.

Procedury związane z rozpatrywaniem wniosków składanych przez osoby, których dotyczą dane osobowe przetwarzane przez Administratora szczegółowo uregulowane zostały w dokumencie pn. Rozpatrywanie wniosków – instrukcja stanowiącym Załącznik nr 6b do niniejszej Polityki bezpieczeństwa.

IX. Reagowanie na incydenty

Procedury związane z reagowaniem na incydenty rozumiane jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych szczegółowo uregulowane zostały w dokumencie pn. Reagowanie na incydenty – instrukcja stanowiącym załącznik nr 7 do niniejszej Polityki bezpieczeństwa.

X. Obszary przetwarzania danych

Administrator sporządził wykaz budynków, pomieszczeń i części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, który stanowi Załącznik nr 8 do niniejszej Polityki bezpieczeństwa.

XI. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

U Administratora nie dochodzi do przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych w rozumieniu RODO. Administrator podjął niezbędne starania o to, aby w przypadku współpracy z podmiotami zarejestrowanymi na terytorium państw trzecich nie przekazywać żadnych danych osobowych.

Przekazywanie danych osobowych, czy ich ujawnianie nie jest przez Administratora planowane, aczkolwiek Administrator ma świadomość konieczności wprowadzenia stosownych procedur, gdyby do przypadków takich miało dochodzić w przyszłości. Procedury zostaną opracowane i wdrożone przed pierwszym planowanym przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

XII. Weryfikacja procedur

Administrator dokonuje weryfikacji postanowień niniejszej Polityki bezpieczeństwa oraz procedur nią przewidzianych nie rzadziej niż raz na rok. Ewentualne wystąpienie incydentu w zakresie ochrony danych osobowych skutkować musi obligatoryjną niezwłoczną weryfikacją przyjętych u Administratora norm. Postanowienia Polityki bezpieczeństwa będą

przystosowywane do zmian wynikających z potrzeb Administratora danych, przemian prawnych oraz rozwoju techniki.

XIII. Postanowienia końcowe

Niniejsza Polityka bezpieczeństwa wraz z wszystkimi załącznikami stanowiącymi jej integralną część przyjęta została uchwałą Zarządu z dnia _____ 2018 r.