POLITYKA OCHRONY DANYCH OSOBOWYCH w Olmet Sp. z o.o. Sp. k.

II. PODSTAWOWE INFORMACJE.

A. CEL POLITYKI I PODSTAWA PRAWNA.

1. Niniejszy dokument zatatuowany „Polityka ochrony danych osobowych" (dalej zwana POLITYKĄ) opisuje działania organizacyjne i techniczne podejmowane przez **Olmet Spółkę z ograniczoną odpowiedzialnością spółkę komandytową z siedzibą w Tarnowskich Górach przy ul. Towarowej 15, 42 – 600 Tarnowskie Góry, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Gliwicach X Wydział Gospodarczy pod numerem KRS 0000380781, NIP 645-252-28-00, REGON: 241895473** (dalej zwana Spółką) jako Administratora Danych Osobowych, których celem jest osiągnięcie i utrzymanie akceptowalnego poziomu bezpieczeństwa przetwarzanych danych osobowych oraz podniesienie poziomu świadomości pracowników w zakresie ochrony tych danych/informacji.
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – 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 dyrektywny 95/46.WE.
3. Celem Polityki jest opisanie działań mających na celu ochronę danych osobowych oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby prawidłowo wykonać obowiązki Administratora w zakresie zabezpieczenia danych osobowych.
4. Do wyznaczonego celu Administrator dąży poprzez wdrożenie odpowiedniego systemu ochrony danych osobowych przed zagrożeniami wewnętrznymi i zewnętrznymi.
5. Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest zarząd Olmet Sp. z o.o.- komplementariusza Olmet Sp. z o.o. Sp. k. a w ramach zarządu Pan Przemysław Oleś, któremu powierzono nadzór nad obszarem ochrony danych osobowych.

B. DEFINICJE.

a) **Administrator -** rozumie się przez to Olmet Spółkę z ograniczoną odpowiedzialnością spółkę komandytową z siedzibą w Tarnowskich Górach.
b) **Osoba upoważniona -** każda osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora;
c) **Użytkownik systemu -** każda osoba, posiadająca upoważnienie do przetwarzania danych osobowych wydane przez Administratora zarejestrowana w systemie /posiadająca unikalny identyfikator i hasło/ przetwarzająca dane osobowe;
d) **Dane osobowe -** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio;
e) **Szczególne kategorie danych osobowych** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, a także dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa ;
f) **Zbiór danych -** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
g) **Przetwarzanie danych -** operację 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;

h) **Obszar Przetwarzania Danych Osobowych –** budynki, pomieszczenia oraz części pomieszczeń, w których przetwarzane są Dane Osobowe;
i) **Usuwanie danych -** zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
j) **Identyfikator użytkownika -** ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
k) **Hasło -** ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
l) **Uwierzytelnianie -** to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
m) **Bezpieczeństwo informacji -** zachowanie poufności, integralności, dostępności i rozliczalności informacji;
n) **Poufność -** właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom i podmiotom;
o) **Dostępność -** właściwość polegającym na byciu dostępnym i użytecznym na żądanie upoważnionego podmiotu lub upoważnionej osoby;
p) **Integralność** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
q) **Rozliczalność -** właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
r) **Naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
s) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
t) **Szkodliwe oprogramowanie** – oprogramowanie, którego celem jest umożliwienie uzyskania nieuprawnionego dostępu do systemu informatycznego;
u) **Zabezpieczanie danych w systemie informatycznym -** wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
v) **Nośnik danych osobowych** – każdy nośnik komputerowy bądź papierowy w postaci akt osobowych oraz ich kserokopie, przenośne urządzenia robocze (laptopy lub inne urządzenia), elektroniczne nośniki informacji (dyski zewnętrzne, płyty kompaktowe, pendrive itp.) wydruki z systemu informatycznego oraz dyski serwerów i kopii zapasowych.

C. ZDEFINIOWANIE ODPOWIEDZIALNOŚCI.

1. Administratorem jest **Olmet Spółka z ograniczoną odpowiedzialnością spółką komandytową z siedzibą w Tarnowskich Górach przy ul. Towarowej 15, 42 – 600 Tarnowskie Góry, wpisanym do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Gliwicach X Wydział Gospodarczy pod numerem KRS 0000380781, NIP 645-252 28 00 ~~100-51-55~~, REGON: 241895473**.
2. Polityka obowiązuje wszystkich pracowników Administratora oraz osoby pracujące na rzecz Administratora na podstawie umów cywilnoprawnych oraz na podstawie prowadzonej działalności gospodarczej.
3. Do obowiązków zarządu Spółki należy zrozumienie oraz zapewnienie świadomości

bezpieczeństwa przetwarzania danych osobowych, jego problematyki i wymagań.

4. Do obowiązków zarządu należy m.in.
   a) podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych;
   b) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych;
   c) wprowadzenie procedur mających na celu prawidłowe i legalne przetwarzanie danych osobowych;
   d) zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa danych osobowych.
5. Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy m.in. :
   a) przetwarzanie danych zgodnie z obowiązującymi przepisami prawa;
   b) zachowanie w tajemnicy danych osobowych oraz informacji o sposobie ich zabezpieczenia;
   c) postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;
   d) informowanie o wszelkich podejrzanych naruszeniach oraz zauważonych naruszeniach dot. Przetwarzania lub zabezpieczenia danych osobowych.

III. POLITYKA BEZPIECZEŃSTWA - ZASADY OGÓLNE.

A. ZAKRES STOSOWANIA POLITYKI

1. Informacje w Spółce przetwarzane i składowane są zarówno w postaci dokumentacji papierowej jak i elektronicznej.
2. Niniejszą Politykę stosuje się m.in. do:
   a) danych osobowych przetwarzanych w systemie informatycznym;
   b) danych osobowych przetwarzanych w trybie tradycyjnym (dokumentacja papierowa);
   c) wszystkich informacji dotyczących pracowników Spółki w tym danych osobowych personelu i treści zawieranych umów o pracę;
   d) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji;
   e) rejestru osób dopuszczonych do przetwarzania danych osobowych;
   f) danych osobowych osób fizycznych będących klientami lub kontrahentami Spółki.

B. ZASADY OGÓLNE PRZETWARZANIA DANYCH OSOBOWYCH.

1. Dane osobowe przetwarzane są z poszanowanie następujących zasad:
   a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   b) rzetelnie i uczciwie (rzetelność);
   c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
   d) w konkretnych celach (minimalizacja);
   e) z dbałością o prawidłowość działań (prawidłowość);
   f) nie dłużej niż potrzeba (czasowość) ;
   g) nie więcej niż potrzeba (adekwatność);
   h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo);
   i) poprzez nieudostępniania danych nieupoważnionym osobom;
   j) poprzez zapewnienie, że działania mogą być przypisane w sposób jednoznaczny tylko jednej osobie;
   k) poprzez przydzielanie praw dostępu do danych osobom tylko i wyłącznie w zakresie niezbędnym do wykonywania czynności służbowych;

l) poprzez nierealizowanie zadań krytycznych z punktu widzenia bezpieczeństwa danych przez tą samą osobę

C. OPIS STRUKTUR ZBIORÓW DANYCH OSOBOWYCH.

1. Zbiory danych osobowych przetwarzanych w Spółce mają następujące struktury:
   a) W zbiorze danych Klientów i kontrahentów Spółki przetwarzane są dane osobowe w zakresie imienia i nazwiska, NIP, adresu, numeru rachunku bankowego, nazwy banku, numeru telefonu, wiadomości e-mail.
   b) W zbiorze danych Pracowników Spółki przetwarzane są dane w zakresie imienia i nazwiska, płci, imienia ojca, imienia matki, nazwiska rodowego, PESEL, NIP, stanu cywilnego, numeru telefonu, miejsca urodzenia, daty urodzenia, serii i numeru dowodu osobistego, wystawcy dowodu osobistego, adresu zamieszkania, urzędu skarbowego, imienia i nazwiska, daty urodzenia, adresu, PESEL męża(żony) oraz dzieci, nazwy banku, numeru rachunku bankowego, adresu e-mail, wykształcenia.

IV. ZASADY REALIZACJI POLITYKI.

A. INFORMACJE OGÓLE.

1. Każda osoba biorąca udział w przetwarzaniu danych osobowych posiada pisemne, imienne upoważnienie do ich przetwarzania nadane przez Administratora stanowiące polecenie Administratora w rozumieniu art. 29 RODO oraz 32 ust. 4 RODO. Upoważnienie to połączone jest z deklaracją pracownika o zachowaniu w tajemnicy danych osobowych, sposobów ich zabezpieczania jak również zapoznania się z treścią Polityki. (*Wzór pisemnego upoważnienia stanowi załącznik nr 1 do niniejszej Polityki.)*
2. Administrator prowadzi ewidencję osób upoważnionych. *(Wzór ewidencji osób upoważnionych stanowi załącznik nr 2 do niniejszej Polityki.)*
3. Administrator wdrożył stosowne środki organizacyjne i techniczne mające na celu należyte zabezpieczenie danych osobowych.
4. Administrator zabezpiecza zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania poprzez stosowanie następujących zasad:
   a) system informatyczny Administratora jest zabezpieczony przed nieupoważnionym dostępem, utratą, modyfikacją lub zniszczeniem danych poprzez stosowanie haseł do komputera;
   b) sieć internetowa wewnętrzna jest zabezpieczona przed nieupoważnionym dostępem z zewnątrz;
   c) każdy pracownik Administratora dysponuje indywidualnym identyfikatorem, za pośrednictwem którego może korzystać z udostępnianych zasobów i usług. Włączone w systemie informatycznym mechanizmy oraz procedury zapewniają rozliczalność użytkowników zarejestrowanych w systemie;
   d) wszyscy pracownicy Administratora zapoznali się z treścią niniejszej Polityki;
   e) pracownicy Administratora mają obowiązek informowania o wystąpieniu zdarzenia związanego z bezpieczeństwem informacji.
5. W przypadku naruszenia ochrony danych osobowych, zgłoszenie go organowi nadzorczemu powinno:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

6. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
7. Administrator raz w roku podejmuje działania mające na celu testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania w postaci audytu sprawdzającego.
8. Administrator wdrożył środki zapewniające zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego w postaci tworzenia kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym oraz programów i narzędzi służących do przetwarzania danych osobowych.
9. Administrator prowadzi rejestr czynności przetwarzania. (*Wzór rejestru czynności przetwarzania stanowi załącznik nr 3 do niniejszej Polityki.)*
10. Szczególną uwagę Administrator zwraca na elementy zarządzania, które mają istotny wpływ na bezpieczeństwo danych rozumiane jako ochrona przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Dotyczy to nie tylko danych osobowych przechowywanych w bazach danych, dokumentacji papierowej, ale również tych danych, które przesyłane są w sieciach komputerowych (w wiadomościach e-mail oraz z baz danych do użytkowników).
11. Administrator przetwarza dane osobowe w swojej siedzibie w Tarnowskich Górach w pomieszczeniach znajdujących się w budynku położonym przy ul. Towarowej 15 oraz w oddziale w Rybniku w budynku położonym przy ul. Podmiejskiej 95, w oddziale w Mszanie w budynku położonym przy ul. Wodzisławskiej 22 oraz w oddziale w Chorzowie w budynku położonym przy ul. Żelaznej 9a.
12. Dostęp do danych osobowych przetwarzanych w systemach informatycznych poprzez sieć telekomunikacyjną mogą mieć wybrane osoby wyłącznie za zgodą Administratora.
13. Administrator przetwarza dane osobowe osób fizycznych w systemach informatycznych oraz w postaci papierowej. Wszystkie dane osobowe przetwarzane przez Administratora są przetwarzane zgodnie z obowiązującymi przepisami prawa.
14. Administrator stosuje zróżnicowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

B. KONTROLA WEJŚCIA.

1. Dostęp dla gości Administratora jest dostępny wyłącznie w konkretnych celach w szczególności w związku z umówionymi spotkaniami.
2. W siedzibie Administratora zabronione jest używanie sprzętu fotograficznego, video oraz sprzętu rejestrującego bez uzyskania zezwolenia od Administratora.

C. DOSTĘP DO POMIESZCZEŃ I POLITYKA KLUCZY.

1. Dostęp do pomieszczeń Administratora, w których odbywa się przetwarzanie danych osobowych jest ograniczony jedynie do pracowników oraz innych osób upoważnionych przez Administratora. Osoby upoważnione do przebywania w obszarze przetwarzania danych osobowych mogą przebywać w nim wyłącznie w zakresie niezbędnym do wykonania czynności opisanych w upoważnieniu.
2. Klucze wydawane są wyłącznie osobom upoważnionym.

3. Pomieszczenia na czas nieobecności osoby upoważnionej należy zamykać na klucz.
4. Zabrania się pozostawiania kluczy w zamkach drzwi, jak również w miejscach dostępnych dla osób nieupoważnionych podczas chwilowej nieobecności osób upoważnionych.
5. Klucze do pomieszczeń oraz klucze zapasowe przechowywane są w szafie zamykanej na klucz znajdującej się w pomieszczeniu monitorowanym do którego dostęp mają tylko osoby upoważnione.
6. W wyjątkowych sytuacjach Administrator Danych Osobowych wydaje osobie upoważnionej klucz zapasowy. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić Administratorowi.
7. Osoby nieupoważnione mogą przebywać w pomieszczeniu, w którym przetwarzane są dane osobowe wyłącznie w obecności upoważnionego pracownika lub za zgodą Administratora Danych Osobowych. Każdorazowo wyznacza się pracownika do nadzoru personelu zewnętrznego.
8. Po zakończeniu pracy osoby upoważnione do przebywania w pomieszczeniach, w których odbywa się przetwarzanie danych osobowych zobowiązane są do:
    a) wyłączenia oświetlenia;
    b) pozamykania szafek, w których znajdują się dokumenty oraz nośniki elektroniczne zawierające dane osobowe;
    c) zabezpieczenia oraz zamknięcia okien i drzwi.

D. IZOLOWANE OBSZARY PRZYJMOWANIA GOŚCI.

1. Unika się przyjmowania gości przez pracowników Administratora w pomieszczeniach biurowych przy stanowiskach pracy z uwagi na to, że może to prowadzić do przypadkowego wycieku informacji poprzez zapoznanie się z treścią otwartego dokumentu papierowego lub elektronicznego bądź przez podsłuchanie rozmowy pracowników.

E. ZASADY PRZYJMOWANIA KLIENTÓW.

1. Klienci powinni być przyjmowani i obsługiwani wyłącznie w wyznaczonym do tego miejscu.
2. Klienci powinni być obsługiwani pojedynczo co oznacza, że przy jednym stanowisku może znajdować się tylko jeden klient. Stanowiska powinny być oddzielone przegródką.
3. Nieobsługiwani Klienci (stojący w kolejce) powinni znajdować się za wyznaczoną linią.
4. Klienci powinni być obsługiwani w warunkach zapewniający zachowanie poufności.

F. URZĄDZENIA SYSTEMU INFORMATYCZNEGO.

1. Administrator posiada własną serwerownię.
2. W działalności Administratora wykorzystywane są urządzenia przenośne: komputery przenośne, nośniki zewnętrzne (pendrive, dyski zewnętrzne), smartfony. Są one użytkowane ze szczególną ostrożnością poza obszarem przetwarzania danych. Zasady korzystania z urządzeń przenośnych
3. Zasady korzystania z urządzeń w instrukcji. (*Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszej Polityki.)*

G. OGÓLNE ŚRODKI BEZPIECZEŃSTWA.

1. Każdy pracownik, przetwarzający dane osobowe musi posiadać upoważnienie do przetwarzania danych osobowych. Upoważnienie zawiera wszystkie wymagane prawem informacje oraz poziom dostępu do systemu informatycznego Administratora.
2. Najpóźniej w ostatnim dniu pracy anuluje się upoważnienie poprzez odnotowanie tego faktu w Ewidencji osób upoważnionych oraz dokonanie odpowiedniej adnotacji w dokumencie

upoważnienia.
3. Upoważnienia przechowuje się w miejscu, w którym przechowywana jest dokumentacja kadrowa.

H. ZADADA CZYSTEGO BIURKA I CZYSTEGO EKRANU.

1. Informacje pozostawione na biurkach mogą ulec zniszczeniu lub uszkodzeniu, lub też mogą zostać ujawnione poprzez wgląd osób nieuprawnionych, w związku z czym należy przestrzegać następujących zasad:
   a) leżące na biurku dokumenty papierowe w miarę możliwości powinny być odwrócone tekstem do dołu;
   b) dokumenty papierowe oraz inne nośniki informacji jak pendrive, dyski przenośne powinny być przechowywane w zamykanych na klucz szafach w szczególności po godzinach pracy;
   c) wszystkie dokumenty papierowe muszą być niszczone przy pomocy niszczarki;
   d) pieczątki powinny być zamykane w szafkach/szufladach z zamkiem;
   e) dokumenty zawierające wrażliwe dane powinny być zamykane w szafkach z zamkiem;
   f) zabronione jest pozostawić zalogowanych komputerów bez nadzoru;
   g) monitory komputerów powinny być tak ustawione, żeby uniemożliwić podgląd informacji na ekranie osobom nieuprawnionym;
   h) po odejściu od stanowiska pracy pracownik jest zobowiązany do zablokowania komputera uniemożliwiającego skorzystania z niego przez osobę postronną oraz do wyłączenia monitora na czas swojej nieobecności;
   i) poza godzinami pracy urządzenia kopiujące powinny być chronione przed użyciem przez nieuprawnione osoby;
   j) dokumenty zawierające dane osobowe należy natychmiast po wydrukowaniu wyjąć z drukarki;
   k) na pulpicie komputera nie powinny znajdować się pliki w których nazwie znajdują się dane osobowe, pliki takie powinny znajdować się w odpowiednio nazwanych folderach.

I. ZASADY KORZYSTANIA Z SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH.

1. Telefony komórkowe zawierające Dane Osobowe użytkowane są jedynie przez osoby upoważnione do przetwarzania Danych Osobowych.
2. Każdy telefon komórkowy zabezpieczony jest przed dostępem przez osoby nieuprawnione hasłem PIN.
3. Telefony komórkowe przechowywane są w pomieszczeniach, do których dostęp mają wyłącznie osoby upoważnione do przetwarzania Danych Osobowych.
4. Użytkownik może wynieść telefon komórkowy poza obszar Przetwarzania Danych osobowych tylko i wyłącznie w celach służbowych.
5. Użytkownik wynoszący telefon komórkowy poza obszar przetwarzania danych osobowych zobowiązany jest zachować szczególną ostrożność, w tym:
   nie pozostawiać telefonu bez nadzoru oraz nie dopuszczać do sytuacji, w której osoba nieuprawniona miałaby możliwość wglądu do danych zapisanych w telefonie.

J. Powierzenie przetwarzania danych.

1. Administrator przekazuje dane osobowe innym podmiotom. Dochodzi wówczas do powierzenia przetwarzania danych osobowych. W takim przypadku Administrator podejmuje następujące działania:
   a) uwzględnia powierzenie przetwarzania danych osobowych w wykazie zbiorów danych;
   b) umieszcza w umowach zapisy dotyczące powierzenia przetwarzania danych osobowych.
2. Zapisy umowne dotyczące powierzenia przetwarzania danych musza zawierać zapisy o tym, że podmiot przetwarzający:
   a) przetwarza dane osobowe wyłącznie w celu i zakresie określonym w umowie, a także wyłącznie na udokumentowane polecenie administratora;
   b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   c) przekazuje powierzone dane osobowe innym podmiotom do przetwarzania tylko po uzyskaniu wyraźnej zgody administratora;
   d) pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
   e) pomaga administratorowi wywiązać się z obowiązków dotyczących zgłaszania naruszeń ochrony danych osobowych oraz w zakresie oceny skutków przetwarzania dla danych osobowych;
   f) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
   g) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

K. Kontrola dostępu do informacji.

1. Pracownicy nie mogą, bez upoważnienia Administratora, udzielać następujących informacji:
   a) o danych osobowych oraz innych informacji o charakterze poufnym;
   b) o zabezpieczeniach, w tym o zabezpieczeniach systemu informatycznego.
2. Ochronie podlega także informacja głosowa, faksowa oraz wizualna. Dla zabezpieczenia przekazywanej informacji wprowadza się następujące wymogi:
   a) zachowanie szczególnej ostrożności podczas prowadzenia rozmów telefonicznych, a w szczególności zakaz przekazywania informacji poufnych i danych osobowych drogą telefoniczną;
   b) zakaz prowadzenia poufnych rozmów w miejscach publicznych (restauracje, publiczne środki transportu, itp.), szeroko dostępnych biurach, pomieszczeniach o cienkich ścianach;
   c) nie pozostawianie wiadomości zawierających treści poufne na „sekretarkach automatycznych”.

V. Postanowienia końcowe

1. Polityka wchodzi w życie z dniem 25 maja 2018 roku.
2. Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
3. Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz faktycznymi zmianami w Spółce, które mogą powodować że zasady ochrony danych osobowych określone w niniejszej Polityce są nieaktualne.
4. W sprawach nieuregulowanych niniejszą Polityką zastosowanie ma RODO – 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 dyrektywny 95/46.WE.