POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W firmie

"Leonardo" Usługi Konsulting Robert Mikołajczyk

ul. Piłsudskiego 36/20

25-431 Kielce

Drukarnia:

"Leonardo" Usługi Konsulting Robert Mikołajczyk

ul. Karczówkowska 5a/10, 25-019 Kielce

Polityka Bezpieczeństwa w zakresie danych osobowych

ROZDZIAŁ I

Postanowienia ogólne

§ 1

1. Polityka bezpieczeństwa zwana dalej „Polityką", określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, sposób przepływu danych pomiędzy poszczególnymi systemami, zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar (jeżeli występują), w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.

2. Instrukcja została opracowana zgodnie z wymogami określonymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu 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 (Dz. U. Nr 100, poz. 1024), ze szczególnym uwzględnieniem jego § 4.

§ 2

1. Ilekroć w Polityce jest mowa o:

1) **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

2) **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

3) **systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

4) **Administratorze Danych** - rozumie się przez to "Leonardo" Usługi Konsulting Robert Mikołajczyk, ul. Piłsudskiego36/20, 25-431 Kielce. Administrator Danych jest osobą nadzorującą przestrzeganie zasad ochrony, która jest obowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochron. W szczególności powinna ona zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmian, utrat, uszkodzeniem lub zniszczeniem. Do jej obowiązków należy między innymi podejmowanie odpowiednich działań w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych, a także nadzór i kontrola w zakresie określonym przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi.

5) **osobie odpowiedzialnej za prawidłowe funkcjonowanie sprzętu, oprogramowania i jego konserwację** - rozumie się przez to informatyka odpowiedzialnego za powyższe zadania wyznaczonego przez Właściciela, zwanego dalej „Informatykiem" (jeżeli występuje). W przypadku gdy Informatyk nie występuje jego obowiązku przejmuje Administrator Danych.

6) **komórce organizacyjnej** - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z regulaminem organizacyjnym,

7) **użytkowniku** – rozumie się przez to osobę wyznaczoną przez Administratora, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadającą ustalony identyfikator i hasło,

8) **pomieszczeniach** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

§ 3

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

2. Zastosowane zabezpieczenia gwarantują:

a) **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

b) **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
c) **rozliczalność** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
d) **integralność systemu** - rozumie się przez to nienaruszalność systemu, niemożność jakiejkolwiek manipulacji,
e) **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

2. Za przestrzeganie zasad ochrony i bezpieczeństwa danych w komórkach organizacyjnych odpowiedzialny jest Administrator Danych.

§ 4

1. Realizację zamierzeń określonych w § 3 ust. 2 powinny zagwarantować następujące założenia:

a) wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych,
b) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
c) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia,
d) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
e) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
f) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
g) śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:

a) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
b) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmian zawartości danych, utrat całości lub części danych),
c) naruszenie lub próby naruszenia integralności systemu,
d) zmianę lub utratę danych zapisanych na kopiach zapasowych,

e) naruszenie lub próby naruszenia poufności danych lub ich części,
f) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
g) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
h) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych,
i) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.

2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II

Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych

§ 6

1. Każdy nowo zatrudniany pracownik - przed dopuszczeniem do dostępu do danych osobowych – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.

2. Wszyscy użytkownicy podlegają okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmian wewnętrznych regulacji.

§ 7

1. Za organizację szkoleń, odpowiedzialny jest Administrator Danych.

2. Szkolenia odbywają się na wniosek Administratora Danych.

§ 8

1. Użytkownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.

W tym celu należy:

a) zwracać szczególną uwagę przy wchodzeniu i wychodzeniu z obiektu na podejrzane osoby lub samochody parkujące w pobliżu,
b) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
c) informować Administratora Danych o podejrzanych osobach, tj.:
   - osobach zachowujących się nienormalnie np. nieodpowiednio ubranych do pory roku, dnia i pogody;
   - osobach przebywających w obiekcie bez wyraźnego celu;
   - osobach posiadających przy sobie podejrzane bagaże, w których mogą być ukryte niebezpieczne przedmioty;
d) przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy a także po jej zakończeniu.

2. Użytkownicy zobowiązani są, na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Danych projekty i propozycje stosownych rozwiązań, których celem jest zabezpieczenie przed naruszeniem ochrony danych osobowych.

§ 9

1. Do podstawowych zabezpieczeń przed naruszeniem ochrony danych osobowych należą:

a) ochrona obiektu przez wszystkie dni w roku,
b) wydzielanie pomieszczeń ,
c) ograniczanie i monitorowanie dostępu do bazy danych,
d) zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami,

§ 10

1. Klucze do pomieszczeń wydawane są wyłącznie osobom do tego uprawnionym.

ROZDZIAŁ III

Przetwarzanie danych osobowych

§ 12

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego odbywa się wyłącznie na obszarze wyznaczonym przez Administratora Danych.

2. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Danych.

3. Szczegółowy wykaz pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe określa załącznik Nr 1 do Polityki.

§ 13

1. W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić, aby:

a) drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby,
b) wydawanie kluczy użytkownikom do pomieszczeń podlegało rejestracji,
c) pomieszczenia, w których znajdują się serwery były wyposażone w miarę możliwości w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej,
d) pracownicy Administratora Danych są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń , w których przetwarzane są dane osobowe,
e) przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych.

§ 14

1. Stały dostęp do pomieszczeń , w których przetwarzane są dane osobowe, mają tylko użytkownicy oraz Informatyk.

2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Administratora Danych.

3. Zakaz wyrażony w ust. 2 dotyczy innych, niż określeni w ust. 1, pracowników Administratora Danych oraz pracowników służb technicznych, porządkowych, itp.

4. Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych.

§ 15

1. W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych jest zabronione.

§ 16

1. Administrator Danych jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa danych osobowych.

2. W celu sprawnego wykonywania swoich zadań Administrator Danych jest uprawniony do wyznaczania użytkownikom określonych zadań.

3. Użytkownicy zobowiązani są do przestrzegania przepisów o ochronie danych osobowych na terenie podległych komórek organizacyjnych, a także do ścisłej współpracy z Administratorem Danych. W tym celu zobowiązani są do:

a) pisemnego wnioskowania o rejestrację nowych zbiorów danych osobowych,
b) okresowego składania pisemnej informacji z przebiegu bieżącej kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
c) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

§ 17

1. Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania określa załącznik Nr 2 do Polityki.

§ 18

1. Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych określa załącznik nr 3 i nr 4 do Polityki.

ROZDZIAŁ IV

Kontrola przestrzegania zasad zabezpieczenia ochrony danych osobowych

§ 19

1. Administrator Danych sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych.

2. Administrator Danych lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.

3. Przedmiotem kontroli, o których mowa w ust. 2 powinno być w szczególności:

a) funkcjonowanie zabezpieczeń systemowych,
b) prawidłowo funkcjonowania mechanizmów kontroli dostępu do zbioru danych,
c) funkcjonowanie zastosowanych zabezpieczeń fizycznych,
d) zasady przechowywania kartotek,
e) zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych,
f) realizacja procedur wdrożonych przez Administratora Danych w zakresie ochrony danych.

4. Administrator Danych prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.

5. Z kontroli, o których mowa w ust. 2 należy sporządzać protokoły, które przechowuje Administrator Danych.

ROZDZIAŁ V

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 20

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Danych

3. Obowiązek określony w ust. 2 ciąży równie na pozostałych pracownikach Administratora Danych.

§ 21

1. Do czasu przybycia Administratora Danych lub upoważnionej przez niego osoby, zgłaszający:

a) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
b) zabezpiecza elementy systemu informatycznego, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
c) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 22

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Administrator Danych lub osoba przez niego upoważniona, po przybyciu na miejsce:

a) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń , a także identyfikuje wielkość negatywnych następstw incydentu,
b) wysłuchuje relacji osoby, która dokonała powiadomienia,
c) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

§ 23

1. Administrator Danych lub upoważniona przez niego osoba sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:

a) dacie i godzinie powiadomienia,
b) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,
c) sytuacji, jaką zastał,
d) podjętych działaniach i ich uzasadnieniu.

§ 24

1. Administrator Danych lub osoba przez niego upoważniona podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:

a) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
b) relacjonuje Administratorowi przedsięwzięte czynności,

c) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych dyscypliny pracy, podjęte zostają stosowne działania wobec osób, które dopuściły się tego uchybienia.

§ 25

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Danych lub osoby przez niego upoważnionej.

2. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Administratora Danych lub upoważnioną przez niego osobę, a w przypadku kradzieży występuje o powiadomienie jednostki policji.

3. W sytuacji, o której mowa w ust. 1 Administrator Danych lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt.

4. W przypadku kradzieży komputera razem z nośnikiem magnetycznym Administrator Danych lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

§ 26

1. Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki bezpieczeństwa oraz przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie Pracy, Kodeksie Pracy oraz wynikającą z ustawy o ochronie danych osobowych.

ROZDZIAŁ VI

Postępowanie w wypadku klęski żywiołowej

§ 27

1. Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień , huragan, woda lub ich przejawami.

§ 28

1. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń , w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

2. O zagrożeniu, jego skali i podjętych krokach zaradczych użytkownik zobowiązany jest niezwłocznie powiadomić Administratora Danych lub osobę przez niego upoważnioną w każdy możliwy sposób. W razie niemożności skontaktowania się z nim użytkownik zawiadamia, co najmniej jedną z niej wymienionych osób:

a) osobę wyznaczoną przez Administratora,
b) Administratora.

2. Numery telefonów Administratora Danych i osób, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

§ 29

1. Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń w których przetwarzane są dane osobowe bez dopełniania obowiązku, o którym mowa w § 14 ust.2 Polityki.

§ 30

1. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do zamknięcia systemu informatycznego,

§ 31

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.

2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

ROZDZIAŁ VII

Postanowienia końcowe

§ 32

1. Polityka jest dokumentem wewnętrznym, zawiera dane, których ujawnienie mogłoby spowodować utratę danych chronionych w związku z czym nie może być udostępniania osobom nieupoważnionym w żadnej formie.

§ 33

1. Administrator Danych jest zobowiązany zapoznać z treścią Polityki każdego użytkownika.

2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, i został zaznajomiony z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3. Oświadczenia przechowywane są w aktach personalnych pracownika.

§ 34

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.

2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

Załącznik nr 1 do Polityki Bezpieczeństwa – Szczegółowy wykaz pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe

Szczegółowy wykaz pomieszczeń tworzących obszar w którym przetwarzane są dane osobowe

Lokalizacja	Nazwa zbioru	Osoby upoważnione
Siedziba firmy: "Leonardo" Usługi Konsulting Robert Mikołajczyk ul. Piłsudskiego 36/20, 25-431 Kielce Drukarnia: "Leonardo" Usługi Konsulting Robert Mikołajczyk ul. Karczówkowska 5a/10, 25-019 Kielce	Klienci sklepu internetowego	Administrator Danych, osoby upoważnione
Siedziba firmy: "Leonardo" Usługi Konsulting Robert Mikołajczyk ul. Piłsudskiego 36/20, 25-431 Kielce Drukarnia: "Leonardo" Usługi Konsulting Robert Mikołajczyk ul. Karczówkowska 5a/10, 25-019 Kielce	Klienci z portalu Allegro.pl	Administrator Danych, osoby upoważnione

Załącznik nr 2 do Polityki Bezpieczeństwa – Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Nazwa zbioru	Zawartość pól informacyjnych	Użytkownicy przetwarzający dany zbiór	Program wykorzystywany do przetwarzania danego zbioru
Klienci sklepu internetowego	Imię, nazwisko, adres zamieszkania, adres email, telefon	Administrator Danych, osoby upoważnione	Przeglądarka internetowa: - Google Chrome - Mozilla Firefox - Internet Explorer - Safari Klient pocztowy: - Mozilla Thunderbird - Windows Live Mail - MS Outlook Oprogramowanie dedykowane: Fit Faktura
Klienci z portalu Allegro.pl	Imię, nazwisko, adres zamieszkania, adres email, telefon	Administrator Danych, osoby upoważnione	Przeglądarka internetowa: - Google Chrome - Mozilla Firefox - Internet Explorer - Safari Klient pocztowy: - Mozilla Thunderbird - Windows Live Mail - MS Outlook Oprogramowanie dedykowane: Fit Faktura

Załącznik nr 3 do Polityki Bezpieczeństwa – Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Nazwa zbioru	Zawartość pól informacyjnych	Użytkownicy przetwarzający dany zbiór	Program wykorzystywany do przetwarzania danego zbioru
Klienci sklepu internetowego	Imię, nazwisko, adres zamieszkania, adres email, telefon	Administrator Danych, osoby upoważnione	Przeglądarka internetowa: - Google Chrome - Mozilla Firefox - Internet Explorer - Safari Klient pocztowy: - Mozilla Thunderbird - Windows Live Mail - MS Outlook Oprogramowanie dedykowane: Fit Faktura
Klienci z portalu Allegro.pl	Imię, nazwisko, adres zamieszkania, adres email, telefon	Administrator Danych, osoby upoważnione	Przeglądarka internetowa: - Google Chrome - Mozilla Firefox - Internet Explorer - Safari Klient pocztowy: - Mozilla Thunderbird - Windows Live Mail - MS Outlook Oprogramowanie dedykowane: Fit Faktura

Załącznik nr 4 do Polityki Bezpieczeństwa – Sposób przepływu danych pomiędzy poszczególnymi systemami

Sposób przepływu danych pomiędzy poszczególnymi systemami

Zbiór danych osobowych	Rodzaj systemu/programu	Sposób współpracy
Klienci sklepu internetowego	MANUALNY	Brak przepływu danych
Klienci z portalu Allegro.pl	MANUALNY	Brak przepływu danych

Załącznik nr 5 do Polityki Bezpieczeństwa – Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

I. Środki ochrony fizycznej danych:

a) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych,

II. Środki sprzętowe, informatyczne i telekomunikacyjne:

a) Oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie.

b) Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem hasła.

c) Dostęp do systemu operacyjnego komputera, z którego są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem hasła o minimalnych wartościach.

d) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

III Środki organizacyjne:

a) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

b) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy.

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