Polityka bezpieczeństwa

przetwarzania danych osobowych w

Chem-Line Trade Sp. z o.o. z/s w Terespolu

Rozdział 1

Postanowienia ogólne

§1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w Chem-Line Trade Sp. z o.o. z/s w Terespolu (zwana dalej: Spółką) jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§2

1. Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

   - Rozporządzeniu 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) /Dz. Urz. UE.L nr 1 19,z 04/05/2016,str. l/,zwanego „rozporządzeniem 2016/679" .

   - Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych /Dz. U. z 2018 r., poz. 1000/.

2. Spółka zapewnia zgodność przetwarzania danych osobowych z regulacjami RODO oraz krajowymi przepisami dotyczącymi ochrony danych osobowych -szczególnie w odniesieniu do: pracowników i kontrahentów firmy, a ponadto danych osobowych powierzonych do przetwarzania podmiotom trzecim, poprzez stosowanie postanowień Polityki oraz zapewnienie technicznych i organizacyjnych środków ochrony danych.

3. Zakres przedmiotowy stosowania niniejszej Polityki obejmuje wszystkie zbiory danych osobowych oraz czynności przetwarzania realizowane przez administratora -odnosi się swoją treścią do informacji:

   a) w formie papierowej -przetwarzanej w ramach tradycyjnego obiegu dokumentów;

   b) w formie elektronicznej -przetwarzanej w ramach systemów informatycznych.

§3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka

naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Spółce rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

a) poufność danych rozumianą jako właściwość zapewniającą, że dane nie są udostępniane osobom nieupoważnionym;

b) integralność danych — rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

c) rozliczalność danych — rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;

d) integralność systemu — rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

e) dostępność informacji — rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

f) zarządzanie ryzykiem rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§5

1. Administratorem danych osobowych przetwarzanych w Spółce jest Grzegorz Kamiński jako Prezes Zarządu.

2. Administrator danych w szczególności:

a) Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

b) Jeżeli obowiązek ten ma zastosowanie – prowadzi rejestr czynności przetwarzania.

c) Jeżeli obowiązek ten ma zastosowanie – wyznacza Inspektora Ochrony Danych (IOD).

Rozdział 2

Definicje

§6

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) administrator danych osobowych (ADO) — oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

2) ustawa — ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000);

3) 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 /Dz. Urz. UE.L nr 119, str. 1/;

4) dane osobowe — to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą), czyli osobie, którą można bezpośrednio lub pośrednio zidentyfikować na podstawie identyfikatora, takiego jak nazwa, imię i nazwisko, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy, jeden lub więcej czynników fizycznych, fizjologicznych, genetycznych, umysłowych, ekonomicznych, kulturowych lub społecznych, danej osoby fizycznej;

5) zbiór danych osobowych — uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów;

6) przetwarzane danych — to dowolna operacja lub zestaw operacji wykonywanych w sposób zautomatyzowany lub niezautomatyzowany, wykonywana na danych osobowych, w szczególności: zbieranie, rejestrowanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, wyszukiwanie, wykorzystanie, ujawnienie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, łączenie, usuwanie lub niszczenie danych osobowych;

7) system informatyczny — zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

8) system tradycyjny zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze;

9) zabezpieczenie danych w systemie informatycznym — wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

10) administrator systemu informatycznego — osoba, upoważniona przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;

11) odbiorca — osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia;

12) strona trzecia — osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe;

13) identyfikator użytkownika (login) — ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

14) hasło — ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3

Zakres stosowania

§7

1. W Spółce przetwarzane są dane osobowe:
    a) kontrahentów /osób fizycznych lub prawnych będących stroną transakcji handlowych;
    b) osób świadczących usługi: ubezpieczeniowe, transportowe, magazynowe, finansowe, remontowe, napraw i konserwacji;
    c) pracowników;
    d) kandydatów do pracy, zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Innymi dokumentami regulującymi ochronę danych osobowych w Spółce są:
    a) ewidencja osób upoważnionych do przetwarzania danych osobowych,
    b) rejestr czynności przetwarzania danych osobowych,
    c) procedura postępowania w przypadku naruszenia ochrony danych osobowych.

§8

Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemach komputerowych obsługujących sprzedaż, realizację inwestycji/zamówień, kadry, płace,

2) wszystkich informacji dotyczących danych osobowych określonych w § 7 ust. 1,

3) odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy: zlecenia, o dzieło, prowadzenia ksiąg rachunkowych,

4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,

5) rejestru osób mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,

6) innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:

   a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

   b) wszystkich lokalizacji — budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,

   c) wszystkich pracowników i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 4

Wykaz zbiorów danych osobowych

§10

1. Dane osobowe gromadzone są w szczególności w następujących zbiorach (jeżeli takowe są aktualnie prowadzone):

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych,
2. Akta osobowe pracowników,
3. Zbiory informacji o pracownikach, oświadczenia na potrzeby ZFŚS,
4. Ewidencja zwolnień lekarskich,

5. Skierowania na badania okresowe, specjalistyczne,
6. Ewidencja urlopów, czasu pracy, wyjść,
7. Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej,
8. Rejestr delegacji służbowych,
9. Listy płac pracowników,
10. Deklaracje ubezpieczeniowe pracowników,
11. Deklaracje i kartoteki ZUS pracowników,
12. Deklaracje podatkowe pracowników,
13. Rejestr wypadków,
14. Umowy cywilno-prawne,
15. Umowy zawierane z kontrahentami,
16. Rejestr klientów,
17. Dokumenty archiwalne.

§ 11

Zbiory o których mowa w § 10 prowadzone są w sposób tradycyjny (papierowy) lub elektroniczny z poszanowaniem zasad ich zabezpieczenia.

Rozdział 5

Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych.

§12

l. Dane osobowe przetwarzane są w budynku, mieszczącym się w Płocku przy ulicy Dworcowej 15 (w tym pomieszczenia, w których: przetwarzane są dane osobowe, znajdują się komputery stanowiące element systemu informatycznego, przechowuje się wszelkie nośniki informacji zawierające dane osobowe w tym: szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwer i inne urządzenia komputerowe, składowane są uszkodzone komputerowe nośniki danych, archiwum).

Rozdział 6

Zasady obowiązujące w Spółce

§ 13

Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:

1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2) dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ("ograniczenie celu");
3) przetwarzanie jest realizowane rzetelnie i uczciwie (rzetelność);
4) administrator przetwarza dane w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
5) dane są zbierane w konkretnych celach i nie "na zapas" (minimalizacja);
6) dane są przetwarzane tylko w celach w jakich zostały zebrane (adekwatność);
7) przetwarzanie jest realizowane z dbałością o prawidłowość danych (prawidłowość);
8) dane są przechowywane nie dłużej niż potrzeba (czasowość);
9) administrator zapewnia bezpieczeństwo danych (bezpieczeństwo).

Rozdział 7

Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§14

1. Zabezpieczenia organizacyjne:
   a) opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych;
   b) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
   c) opracowano i bieżąco prowadzi się rejestr czynności przetwarzania;
   d) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych;
   e) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   f) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   g) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

h) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

i) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści;

j) zawarto umowy powierzenia przetwarzania danych.

2. W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

   a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi;

   b) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem;

   c) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach;

   d) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach;

   e) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy;

   f) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów;

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

3. W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

   a) komputery służące do przetwarzania danych osobowych nie są połączone z lokalną siecią komputerową;

   b) dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła lub dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika lub hasła;

c) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity (stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową);

d) użyto system Firewall do ochrony dostępu do sieci komputerowej;

e) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;

f) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą stosownych urządzeń.

4. Środki ochrony fizycznej:

a) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem lub systemem alarmowym;

b) urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach;

c) dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

Rozdział 8

Zadania administratora danych osobowych

§ 15

Do najważniejszych obowiązków administratora danych osobowych lub administratora bezpieczeństwa informacji należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych,

2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi,

3) przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych — w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych,

4) wydawanie i cofanie upoważnień do przetwarzania danych osobowych, w zbiorach danych w postaci papierowej oraz systemach informatycznych,

5) każda osoba przetwarza dane na polecenia administratora danych osobowych lub na podstawie przepisów prawa,

6) prowadzenie ewidencji osób upoważnionych do przetwarzania,

7) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,

8) nadzór nad bezpieczeństwem danych osobowych,

9) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

10) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych. Sprawowanie kontroli nad prawidłowym dostępem do danych osobowych.

Rozdział 9

Zadania administratora systemu informatycznego.

§ 16

1. Administrator systemu informatycznego odpowiedzialny jest za:

• bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych, • optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego, • instalacje i konfiguracje oprogramowania systemowego, sieciowego, • konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem, • nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, • współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych, • zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego, • zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie, • przeciwdziałanie próbom naruszenia bezpieczeństwa informacji, • przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie, • wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń, • zarządzanie licencjami, procedurami ich dotyczącymi, • prowadzenie profilaktyki antywirusowej.

2. Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych oraz Polityki bezpieczeństwa Spółki przez administratora danych.

Rozdział 10

Postanowienia inne i końcowe

§ 17

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanym na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych.

§ 18

1. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych.
2. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.
4. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
5. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.
6. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.
7. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:
    a) prawo dostępu do danych,
    b) prawo do sprostowania danych,
    c) prawo do usunięcia danych,
    d) prawo do przenoszenia danych,
    e) prawo do sprzeciwu wobec przetwarzania danych,

f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

8. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
9. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.
10. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.