Polityka ochrony danych osobowych

w TSLOGISTIC Tomasz Sawicki

I. Postanowienia wprowadzające

1. Cele i deklaracje

1) Administrator danych osobowych, świadomy wagi zagrożeń jakie niesie ze sobą przetwarzanie danych osobowych dla wolności i praw osób, których dane dotyczą, uznaje ochronę tych danych, w szczególności zapewnienie ich bezpieczeństwa, za jeden z priorytetów działalności TSLOGISTIC Tomasz Sawicki.
2) Administrator danych osobowych podejmuje działania mające na celu wdrożenie przez TSLOGISTIC Tomasz Sawicki przepisów o ochronie danych osobowych oraz zapewnienie stałej zgodności działalności TSLOGISTIC Tomasz Sawicki z tymi przepisami.
3) W celu realizacji zadań określonych w ppkt. 1) i 2) ustanawia się *Politykę ochrony danych osobowych w TSLOGISTIC Tomasz Sawicki.* Niniejszy dokument stanowi politykę ochrony danych w rozumieniu art. 24 ust. 2 Rozporządzenia 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 (dalej RODO).
4) Administrator danych osobowych oczekuje, że zasady i procedury określone w niniejszym dokumencie będą faktycznie wdrożone i stosowane przez ich adresatów. Zobowiązuje się wszystkie osoby dopuszczone do przetwarzania danych osobowych w TSLOGISTIC Tomasz Sawicki do dostosowania ich postępowania do wymogów wynikających z niniejszej *Polityki ochrony danych osobowych.*

2. Zakres stosowania

1) Zasady i procedury określone w niniejszym dokumencie stosuje się zarówno do danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i przetwarzanych w systemach informatycznych.
2) Zasady i procedury określone w niniejszym dokumencie stosuje się do wszystkich osób przetwarzających dane osobowe w ramach TSLOGISTIC Tomasz Sawicki, zarówno do zatrudnionych w TSLOGISTIC Tomasz Sawicki, jak i pozostałych, które zostały dopuszczone do przetwarzania, np. wolontariuszy, praktykantów, itd.

3. Definicje

Ilekroć w polityce bezpieczeństwa danych osobowych jest mowa o:

1) administratorze danych – rozumie się przez to jednoosobową własność prywatną reprezentowaną przez właściciela działalności
2) administratorze systemu – rozumie się przez to dostawcę usług informatycznych
3) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
4) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych,

jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

5) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione, usunięte lub zniszczone w sposób nieautoryzowany,

6) odbiorcy danych – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

   - osoby, której dane dotyczą,
   - osoby upoważnionej do przetwarzania danych,
   - przedstawiciela, o którym mowa w art. 27 RODO,
   - podmiotu przetwarzającego, o którym mowa w art. 28 RODO,
   - organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z przepisami prawa,

7) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

8) pełnomocniku bezpieczeństwa informacji – rozumie się przez to osobę, której administrator danych powierzył realizację zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych,

9) podmiocie przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 28 RODO,

10) raportach – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

11) RODO – rozumie się przez to rozporządzenia 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,

12) rozliczalności – rozumie się przez to właściwość zapewniającą, że podejmowane działania mogą być przypisane w sposób jednoznaczny konkretnej osobie lub podmiotowi,

13) sieci publicznej – rozumie się przez to publiczną sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. DzU z 2014, poz. 243 z późn. zm.),

14) serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

15) systemie informatycznym administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

16) ustawie – rozumie się przez to ustawę z dnia 10.05.2018 r. o ochronie danych osobowych

17) uwierzytelnianiu – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

18) upoważnionym - rozumie się przez to osobę, która została upoważniona do przetwarzania danych osobowych

19) użytkowniku – rozumie się przez to upoważnionego, któremu nadano identyfikator

i przyznano hasło.

II. Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

Administrator danych osobowych reprezentowany przez właściciela działalności gospodarczej realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków;
3) wyznacza pełnomocnika bezpieczeństwa informacji oraz określa zakres jego zadań i czynności w tym do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych, o ile jako właściwy do jej prowadzenia nie zostanie wskazany w niniejszym dokumencie inny podmiot;
4) we współpracy z administratorem systemu i pełnomocnikiem bezpieczeństwa informacji zapewnienie użytkownikom odpowiednich stanowisk pracy umożliwiających bezpieczne przetwarzanie danych;
5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Pełnomocnik bezpieczeństwa informacji

Pełnomocnik bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
2) sprawuje bieżący nadzór nad funkcjonowaniem systemu zabezpieczeń danych osobowych,
3) przeprowadza wewnętrzne audyty (sprawdzenia) przestrzegania przepisów o ochronie danych osobowych, aktualności dokumentacji z zakresu ochrony danych osobowych oraz przestrzegania określonych w niej zasad,
4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
5) zapoznaje się na bieżąco z przepisami dotyczącymi ochrony danych osobowych i wytycznymi organu nadzorczego w tej dziedzinie, dbając o dostosowanie działalności TSLOGISTIC Tomasz Sawicki do aktualnych wymogów.
6) przygotowuje lub zatwierdza dokumenty lub odpowiednie klauzule w dokumentach dotyczące ochrony danych osobowych,
7) prowadzi lub nadzoruje prowadzenie dokumentacji z zakresu ochrony danych osobowych,
8) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych,
9) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
10) występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych,

11) występuje z wnioskiem do administratora systemu o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych,

12) występuje z wnioskami o odwołanie upoważnienia do przetwarzania danych osobowych i/lub wyrejestrowania użytkownika z systemu informatycznego.

13) nadzoruje realizację obowiązku zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie tych danych, w szczególności decyduje o terminach i sposobach przeprowadzenia szkoleń w tym zakresie,

14) w porozumieniu z administratorem danych osobowych na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę.

3. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

3) na wniosek administratora danych osobowych przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,

6) wyrejestrowuje użytkowników na polecenie administratora danych osobowych

7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, pełnomocnikowi bezpieczeństwa informacji lub administratorowi danych,

8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje pełnomocnika bezpieczeństwa informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,

9) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,

10) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Upoważniony

Każdy upoważniony do przetwarzania danych osobowych jest zobowiązany przestrzegać następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania

nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) musi zachować w tajemnicy treść danych osobowych oraz sposób ich zabezpieczenia. Użytkownik jest zobowiązany do zachowania powyższych tajemnic przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*;

4) stosuje się do wydawanych przez administratora danych, pełnomocnika bezpieczeństwa informacji oraz innych przełożonych procedur, wytycznych oraz poleceń służbowych mających na celu zapewnienie zgodnego z prawem przetwarzania danych osobowych;

5) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6) zabezpiecza dane przed ich utratą, nieautoryzowanym zmienieniem lub ujawnieniem osobom nieupoważnionym.

III. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Obszar przetwarzania danych osobowych określa wewnętrzny dokument: „*Opis obszaru przetwarzania”*.

2. Zasoby danych osobowych

1) Na zasoby danych osobowych TSLOGISTIC Tomasz Sawicki składają się zarówno dane osobowe przetwarzane w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i przetwarzanych w systemach informatycznych.
2) Opis zasobów danych osobowych TSLOGISTIC Tomasz Sawicki obejmujący informację o treści i strukturze każdego z zasobów oraz o sposobie przepływu danych pomiędzy zasobami (wewnętrzny dokument: „*Opis zasobów danych osobowych”*).

3. System informatyczny

1) System informatyczny administratora danych opisuje dokument *Instrukcje zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*;
2) Sposób przetwarzania danych osobowych w systemie informatycznym administratora danych określają dokumenty: „*Opis zasobów danych osobowych”* oraz „*Ewidencja czynności przetwarzania”*.

4. Dokumentacja ochrony danych osobowych

1) TSLOGISTIC Tomasz Sawicki prowadzi dokumentację ochrony danych osobowych na którą składają się:
    a. opis obszaru przetwarzania danych osobowych zgodnie z pkt. 1
    b. opis zasobów danych osobowych zgodnie z pkt. 2
    c. ewidencje o których mowa w ppkt. 2)
    d. rejestr czynności przetwarzania

e. dokumentacja audytów o której mowa w ppkt. 3)

f. umowy z podmiotami przetwarzającymi

2) w ramach dokumentacji ochrony danych osobowych prowadzone są następujące ewidencje:

g. pełnomocnik bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz ewidencję udostępnień danych osobowych

h. administrator systemu wraz z pełnomocnikiem bezpieczeństwa informacji prowadzi ewidencję komputerów przenośnych.

3) na dokumentację audytów, których mowa w ppkt. 1 lit. d) składają się:

i. dokumentacja sprawdzeń planowych przeprowadzonych zgodnie z postanowieniami częścią VII pkt. 7 ppkt. 1 niniejszej *Polityki*.

j. dokumentacja sprawdzeń doraźnych zgodna z postanowieniami części VIII pkt. 4.

IV. Identyfikacja zagrożeń bezpieczeństwa danych osobowych

Identyfikuje się następujące zagrożenia bezpieczeństwa danych osobowych przetwarzanych w TSLOGISTIC Tomasz Sawicki:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej, włamanie do budynku;

2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);

3) awarie sprzętu lub oprogramowania, zarówno losowe, jak i spowodowane przez niewłaściwe działanie użytkowników i serwisantów,

4) zastosowanie niewłaściwych metod zabezpieczenia systemu informatycznego lub brak dostosowania poziomu zabezpieczeń do aktualnego poziomu wyzwań technologicznych;

5) działania przestępcze mające na celu przejęcie lub zniszczenie danych osobowych (np. ataki internetowe);

6) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;

7) naruszenia zasad i procedur określonych w dokumentacji ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, będące skutkiem nieprzestrzegania procedur ochrony danych, w tym zwłaszcza:

- wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez wiedzy i zgody administratora danych.

- ujawnienie osobom nieupoważnionym danych osobowych, jak też procedur ochrony danych stosowanych u administratora danych (poprzez umożliwienie wglądu lub przekazania danych i dokumentacji);

- naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie lub zgoda na takie działania przez inne osoby (np. udostępnienie identyfikatora i hasła innemu użytkownikowi);

- niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe),
- przetwarzanie danych osobowych w celach niezgodnych z ich przeznaczeniem,

V. Przeciwdziałanie zagrożeniom bezpieczeństwa danych osobowych (wskazanie działań oraz środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

1. Strefy bezpieczeństwa

1) W siedzibie administratora danych wydzielono strefę bezpieczeństwa klasy II, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tej strefy wchodzą:
   a. pomieszczenie z serwerem, w którym może przebywać wyłącznie administrator systemu oraz inne osoby upoważnione, a osoby postronne w ogóle nie mają dostępu;
   b. pomieszczenie działu administracji i finansów, w którym mogą przebywać pracownicy administracyjno-finansowi, inni użytkownicy danych tylko w towarzystwie pracowników tego działu, a osoby postronne w ogóle nie mają dostępu;
2) W strefie bezpieczeństwa klasy II do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych.

2. Zabezpieczenie sprzętu

1) Administrator systemu wskazuje użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację urządzeń i systemu informatycznego;
2) Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.
3) Bieżąca konserwacja sprzętu administratora danych wykorzystywanego do przetwarzania danych osobowych prowadzona jest przez administratora systemu lub pod ich nadzorem przez innych upoważnionych.
4) Administrator danych w konsultacji z administratorem systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.
5) Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi

także zawiera się umowy powierzenia przetwarzania danych.

3. Zabezpieczenie systemu informatycznego

1) System informatyczny posiada szerokopasmowe połączenie z Internetem.
2) Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.
3) Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domagają się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora systemu oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
4) Administrator systemu w porozumieniu z administratorem danych dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
5) Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące.

4. Kontrola dostępu do systemu i monitorowanie pracy użytkowników

1) Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.
2) W razie potrzeby, po uzyskaniu uprzedniej akceptacji administratora danych, administrator systemu może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.

5. Polityka osobowa

1) Nabór pracowników na stanowiska związane z przetwarzaniem danych osobowych dokonywany jest z uwzględnieniem kompetencji merytorycznych oraz kwalifikacji moralnych kandydatów. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.
2) Dopuszczenie do stanowisk związanych z przetwarzaniem danych osobowych następuje po zrealizowaniu obowiązków wynikających z przepisów prawa oraz niniejszej *Polityki ochrony danych osobowych*, w szczególności po wystawieniu stosownego indywidualnego upoważnienia oraz zapoznaniu osób dopuszczanych do przetwarzania z zasadami dotyczącymi bezpieczeństwa danych osobowych.
3) Ryzyko naruszenia zasad ochrony danych osobowych ze strony osób, które nie zostały upoważnione do przetwarzania danych osobowych (np. personel sprzątający) jest minimalizowane przez odpowiednie przeszkolenie ich (pouczenie) oraz zobowiązywanie do zachowania tajemnicy.

6. Indywidualne wymagania dotyczące użytkowników

Użytkownicy zobowiązani są do zachowania następujących reguł bezpieczeństwa:

1) powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu oraz instalowania nieautoryzowanego oprogramowania, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
2) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
3) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);
4) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
5) przestrzegania indywidualnych uprawnień i realizacji obowiązków w zakresie przetwarzania danych osobowych, w szczególności właściwego korzystania z powierzonych sprzętów i udostępnionych zasobów oraz używania wyłącznie własnego identyfikatora i hasła;
6) odpowiedniego zabezpieczenia identyfikatora i hasła wymaganego do uwierzytelnienia się w systemie oraz nieudostępniania go innym osobom;
7) zachowania danych osobowych i sposobu ich zabezpieczenia w tajemnicy, w tym także wobec osób najbliższych;
8) ustawiania ekranów komputerowych tak, by osoby nieuprawnione nie widziały treści wyświetlanych na ekranie;
9) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
10) niepozostawiania bez kontroli włączonych urządzeń zawierających dane osobowe oraz niezabezpieczonych dokumentów (czasowe opuszczania stanowiska pracy jest dopuszczalne dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu urządzenia w inny sposób);
11) niszczenia niepotrzebnych wydruków i kopii dokumentów po ich wykorzystaniu oraz kasowania po wykorzystaniu danych z dysków przenośnych;
12) zapisywanie plików lub wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
13) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;
14) zadbanie o odpowiednie zabezpieczenie wszelkich dokumentów i wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy (np. w szafie zamykanej na klucz);
15) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
16) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

7. Komputery przenośne i praca poza siedzibą administratora

1) Wynoszenie poza obszar przetwarzania danych urządzeń i dokumentów zawierających dane osobowe jest dopuszczalne jedynie za wiedzą i zgodą

administratora danych lub bezpośredniego przełożonego.

2) Urządzenia zawierające dane osobowe wynoszone poza obszar przetwarzania danych należy chronić przed uszkodzeniami fizycznymi. Należy też bezwzględnie przestrzegać zaleceń producentów dotyczących ochrony sprzętu. W szczególności należy pamiętać, że urządzenia elektroniczne mogą ulec uszkodzeniu w skutek działanie silnego pola elektromagnetycznego i chronić je przed takim oddziaływaniem.

3) Urządzenia przenośne, nośniki danych oraz dokumenty wynoszone poza obszar przetwarzania danych nie powinny być pozostawiane bez nadzoru. W szczególności zabrania się pozostawiania urządzeń i dokumentów zawierających dane osobowe bez odpowiedniego zabezpieczenia w miejscach publicznych, pokojach hotelowych oraz w samochodach.

4) Wykorzystywanie urządzeń przenośnych, nośników danych oraz dokumentów zawierających dane osobowe w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko utraty, zniszczenia lub zapoznania się z danymi przez osoby nieupoważnione. Za miejsca szczególnego ryzyka należy uznać restauracje oraz środki komunikacji publicznej.

5) Niedozwolone jest udostępnianie urządzeń przenośnych i nośników danych należących do administratora danych osobom nieupoważnionym, w tym domownikom i osobom bliskim użytkownika. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych lub chroniącym dostęp do nośników danych.

6) Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa termin i zasady zwrotu sprzętu.

VI. Zapewnienie zgodności działalności TSLOGISTIC Tomasz Sawicki z RODO (przeciwdziałanie ryzyku naruszenia wolności i praw osób, których dane dotyczą)

1. Realizacja zasad ochrony danych osobowych

1) Zasada legalności przetwarzania. Należy zapewnić by dane osobowe były przetwarzane wyłącznie po spełnieniu jednego z warunków dopuszczalności przetwarzania określonych w art.. 6 ust. 1 RODO, a w przypadku szczególnych kategorii danych (tzw. danych wrażliwych) art.. 9 i art. 10 RODO.

2) Zasada rzetelności przetwarzania. Przetwarzanie rzetelne należy rozumieć jako przetwarzanie uczciwie w stosunku do osoby, których dane dotyczą (po angielsku "fair"). Podejmując dowolne czynności przetwarzania należy brać pod uwagę (respektować) prawa i interesy podmiotów danych. Należy wziąć pod uwagę, że przetwarzanie może być dokuczliwe dla podmiotu danych i spróbować zminimalizować te uciążliwości. Nie można też próbować oszukiwać, ani wykorzystywać braku wiedzy lub trudnej sytuacji podmiotu danych.

3) Zasada przejrzystości przetwarzania. Należy zapewnić przejrzystą informację podmiotom danych o dotyczącym ich przetwarzaniu. Powinny być stworzone ścieżki komunikacji umożliwiające zainteresowanym skorzystanie z przyznanych im praw.

4) Zasada ograniczoności celu. Dane wolno zbierać jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie wolno ich przetwarzać po zebraniu w sposób niezgodny z tymi celami. Do celu należy dostosować nie tylko ilość zbieranych

danych, ale też zakres ich przetwarzania oraz okres przez który są przechowywane.

5) Minimalizacja danych. Dane powinny być adekwatne do celu, czyli ograniczone do niezbędnego minimum. Metodą urzeczywistnienia tej zasady może być m.in. pseudonimizacja. Gdy cel przetwarzania tego nie wymaga to w ogóle nie należy dokonywać identyfikacji osobowej.

6) Prawidłowość danych. Dane powinny być prawdziwe (zgodne z prawdą) i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

7) Ograniczenie przechowywania. Dane wolno przechowywać w formie umożliwiającej identyfikację osoby, której one dotyczą, jedynie przez okres niezbędny dla realizacji celów, w których dane te są przetwarzane.

2. Realizacja obowiązków informacyjnych i zapewnienie przejrzystej komunikacji

1) Informacje przekazywane podmiotom danych należy formułować w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

2) Należy uprawdopodobnić, że informacje są przekazywane osobie, której dane dotyczą. W razie wątpliwości należy zażądać dodatkowych informacji w celu zweryfikowania tożsamości, osoby, która się kontaktuje w celu uzyskania informacji.

3) Przekazując informacje podmiotowi danych należy zadbać o to by informacja ta obejmowała wyłącznie dane go dotyczące. Należy dołożyć starań, by informacja przekazywana jednej osobie nie zdradzała informacji o innych.

4) Zbierając informacje bezpośrednio od osoby, której dotyczą należy jednocześnie przekazać tej osobie informacje wskazane w art. 13 ust. 1 i 2 RODO. Obowiązek ten należy zrealizować w trakcie pozyskiwania informacji.

5) Gdy dane są zbierane z innego źródła niż od osoby, której dotyczą to należy spełnić obowiązek informacyjny w zakresie art.. 14 ust. 1 i 2 RODO. Należy to zrobić w rozsądnym terminie (do miesiąca) od zebrania informacji, nie później jednak niż przy pierwszej komunikacji z podmiotem danych lub pierwszym udostępnieniem danych.

6) Stosowną informację w zakresie art.. 13 ust. 1 i 2 lub art.. 14 ust. 1 i 2 RODO należy podmiotowi danych przekazać także w przypadku zmiany celu przetwarzania dokonanym po zebraniu danych, chyba, że został już o tym uprzedzony.

7) Należy zapewnić ścieżki komunikacji umożliwiające osobom, których dane dotyczą kontakt w celu realizacji przyznanych im praw.

3. **Realizacja żądań osób, których dane dotyczą**

1) Jeżeli zainteresowany skorzysta z prawa dostępu do danych (zażąda informacji na temat dotyczącego go przetwarzania) to udziela się mu jej zgodnie z art. 12 ust. 1 i 2 RODO. Jeśli podmiot danych tego zażąda, a jest to możliwe, przekazuje się mu także kopię dotyczących go danych. Informacji na żądanie udziela się zasadniczo w terminie miesiąc, chyba, że sprawa jest skomplikowana. Wtedy przedłużenie terminu następuje zgodni z art. 12 ust. 3 RODO.

2) Jeżeli zainteresowany skorzysta z prawa do sprostowania to na jego żądanie dokonuje się sprostowania nieprawidłowych danych. Prawo to obejmuje też uzupełnienie niekompletnych danych, przy czym kompletność ocenia się z uwzględnieniem celów przetwarzania. O ile to możliwe to o dokonanym sprostowaniu informuje się odbiorców, którym dane zostały przekazane.

3) Jeżeli zainteresowany skorzysta z prawa do usunięcia danych (bycia zapomnianym) to na jego żądanie usuwa się dotyczące go dane, chyba że spełnione są wymogi ich

dalszego przetwarzania z art. 17 ust. 3 RODO. O ile to możliwe to o dokonanym usunięciu informuje się odbiorców, którym dane zostały przekazane. Gdy dane zostały upublicznione należy podjąć starania w celu usunięcia wszelkich łączy do tych danych, ich kopii lub replikacji stworzonych przez innych administratorów.

4) Jeżeli zainteresowany skorzysta z prawa do ograniczenia przetwarzania to na jego żądanie należy ograniczyć przetwarzanie do wskazanych czynności, chyba, że zachodzą przesłanki ich dalszego przetwarzania, w szczególności te wymienione w art. 18 ust. 2 RODO. O ile to możliwe to o dokonanym ograniczeniu informuje się odbiorców, którym dane zostały przekazane.

5) Jeżeli zainteresowany skorzysta z prawa do przeniesienia danych to dostarcza mu się dotyczących go danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Prawo to przysługuje, gdy dane mają postać zapisu elektronicznego i są przetwarzane na podstawie warunku zgody lub realizacji umowy. Na żądanie zainteresowanego dane dostarcza się bezpośrednio wskazanemu przez niego podmiotowi.

6) Jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych osobowych, w tym profilowania, powołując się na swoją szczególną sytuację, to należy zaprzestać dalszego przetwarzania dotyczących go danych, chyba, że spełnione są przesłanki dalszego przetwarzania określone w art. 21 ust. 1 RODO.

7) Jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych w celach marketingowych, w tym profilowania, to nie można nie uwzględnić sprzeciwu.

4. **Zgoda na przetwarzanie danych osobowych**

1) Jeżeli zgodnie z art. 6 ust. 1 lub 9 ust. 1 RODO podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą to przyzwolenie na przetwarzanie danych powinno być dobrowolne, konkretne, świadome i jednoznaczne. Musi spełniać też wymogi rozliczalności i transparentności.

2) Zapewnia się prawo do wycofania zgody.

3) Nie jest dopuszczalne uzależnienie wykonania usługi niezwiązanej bezpośrednio ze zgodą od jej udzielenia.

4) W przypadku usług społeczeństwa informacyjnego oferowanych dziecku podejmuje się wszelkie niezbędne działania by uzyskać aprobatę opiekuna.

5. **Profilowanie**

1) Podejmowanie zautomatyzowanych decyzji wobec indywidualnych osób, w tym profilowanie, jest dopuszczalne wyłącznie w przypadkach określonych w art. 22 ust. 3, w szczególności, gdy zainteresowana osoba wyraziła na to zgodę.

2) Osobie, wobec której są podejmowane zautomatyzowane decyzje lub którą się profiluje zapewnia się:

- prawo do zakwestionowania tej decyzji;

- prawo do wyrażenia własnego stanowiska w przedmiocie podejmowanych wobec niej decyzji i profilowania;

- prawo do uzyskania interwencji ludzkiej, czyli do indywidualnego rozpatrzenia jej sprawy przez administratora danych;

- prawo do wniesienia sprzeciwu zgodnie z art. 21 ust. 1 i 2 RODO.

6. **Udostępnianie danych osobowych**

1) Jeśli zgodnie z przepisami prawa administrator danych jest zobowiązany do

przekazywana danych osobowych wskazanym podmiotom (np. Urzędowi Skarbowemu lub ZUS) to upoważnieni pracownicy administratora danych realizują ten wymóg zgodnie z zakresem swoich obowiązków służbowych stosując się ściśle do wskazanych przepisów.

2) Jeśli do administratora danych wystąpi z wnioskiem o udzielenie informacji osobowej podmiot, który twierdzi, że jest uprawniony do uzyskania takiej informacji na podstawie przepisów prawa udostępnienie informacji może nastąpić jedynie po:

   - zweryfikowaniu podstawy prawnej udostępnienia;

   - zweryfikowaniu czy składający wniosek jest podmiotem za który się podaje;

   - odnotowaniu udostępnienia w ewidencji udostępnień danych osobowych.

   Ewidencję udostępnień danych osobowych prowadzi pełnomocnik bezpieczeństwa informacji.

3) W przypadku, gdy z wnioskiem o którym mowa w ppkt. 2) wystąpi uprawniony funkcjonariusz, w szczególności policji, i wnioskujący stwierdzi, że istnieje konieczność niezwłocznego działania udostępnienie informacji może nastąpić po:

   - wylegitymowaniu funkcjonariusza;

   - na podstawie pisemnego oświadczenia funkcjonariusza lub za pisemnym pokwitowaniem przez niego uzyskania dokumentów.

   Jeśli złożenie oświadczenia lub pokwitowanie uzyskania danych przez funkcjonariusza nie są możliwe ze względu na okoliczności udostępniania, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową. Ewidencjonując udostępnienie pełnomocnik bezpieczeństwa informacji opisze w rubryce „Uwagi" ewidencji udostępnień szczególne okoliczności udostępnienia.

4) Jeśli do administratora danych wystąpi z wnioskiem o udzielenie informacji osobowej podmiot, który nie jest uprawniony do uzyskania takiej informacji na podstawie przepisów prawa udostępnienie informacji może nastąpić jedynie gdy:

   - cel przetwarzania nie ulega zmianie;

   - osobie, której dane mają być udostępnione zostanie umożliwione skorzystanie z prawa sprzeciwu;

   - nastąpi zweryfikowanie tożsamości podmiotu składającego wniosek;

   - udostępnienie zostanie odnotowane w ewidencji udostępnień danych osobowych.

7. **Przekazywanie danych do państw trzecich lub organizacji międzynarodowym**

1) Przekazywanie danych osobowych do państw trzecich jest zasadniczo zabroniona, chyba, że decyzję taką podejmie administrator danych, ze względu na szczególne okoliczności.

2) W przypadku określonym w ppkt. 1) przekazanie jest dokonywane wyłącznie zgodnie z wymogami określonymi w art. 44-50 RODO. Administrator danych dokłada staranności, by zapewnić stopień ochrony osób fizycznych zagwarantowany w RODO.

8. **Współpraca z podmiotami przetwarzającymi**

1) Jeśli wymagają tego okoliczności administrator danych może podjąć decyzje o powierzeniu przetwarzania danych osobowych podmiotowi przetwarzającemu.

2) Wybierając podmiot przetwarzający administrator danych dokłada staranności, by podmiot ten zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO.

3) Powierzenie danych osobowych podmiotowi przetwarzającemu następuje na podstawie pisemnej umowy określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora danych i podmiotu przetwarzającego.

4) Umowa o której mowa w ppkt. 3) zawiera, jeśli to właściwe, w szczególności:

   a. zobowiązanie przetwarzającego do tego, że przetwarzanie danych osobowych będzie się odbywało wyłącznie na udokumentowane polecenie administratora danych,

   b. deklarację przetwarzającego, że osoby upoważnione przez niego do przetwarzania danych osobowych zobowiązały się lub zobowiążą do zachowania w tajemnicy dane osobowe oraz sposób ich zabezpieczenia;

   c. deklarację przetwarzającego, że wdrożył lub wdroży odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa zgodnie z art. 32 RODO,

   d. deklarację przetwarzającego wskazującą, że jeśli korzysta lub będzie korzystać z usług innego podmiotu przetwarzającego, to wypełnia lub wypełni warunki określone w art. 28 ust. 2 i 4 RODO,

   e. zobowiązanie przetwarzającego do pomocy administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w pkt. 1-7,

   f. zobowiązanie przetwarzającego do pomocy administratorowi danych w realizacji obowiązków określonych w częściach VIII i IX niniejszej *Polityki*,

   g. zobowiązanie przetwarzającego do usunięcia lub zwrotu wszelkich danych osobowych administratora oraz wszelkich ich istniejących kopii po zakończeniu świadczenia usług, jeśli administrator danych wystąpi z takim żądaniem.

9. Współadministrowanie

1) Jeśli wymagają tego okoliczności administrator danych może podjąć decyzje o wspólnym ustaleniu celów i sposobów przetwarzania danych osobowych z innym administratorem (tzw. współadministrowanie).

2) Uzgodnienie wskazane w ppkt. 1) jest zawierane w formie umowy pisemnej.

3) Umowa o której mowa w ppkt. 2) w przejrzysty sposób:

   a. określa odpowiednie zakresy odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności obowiązków informacyjnych oraz innych obowiązków względem osób, których dane dotyczą,

   b. wskazuje jak osoby, których dane dotyczą mogą kontaktować się w celu uzyskania informacji i realizacji przysługujących im praw.

4) Umowa o której mowa w ppkt. 1) w zakresie w jakim dotyczy osób, których dane mają być przetwarzane jest udostępniana tym osobom na ich żądanie.

VII. Działania nadzorcze i audyty wewnętrzne.

1. Nadzór nad przestrzeganiem ochrony danych osobowych

1) W celu zapewnienia ochrony wolności i praw osób, których dane dotyczą, a zwłaszcza bezpieczeństwa dotyczących ich danych, pełnomocnik bezpieczeństwa informacji zapewnia zgodność działalności TSLOGISTIC Tomasz Sawicki z przepisami.
2) Realizując zadanie określone w ppkt. 1) pełnomocnik bezpieczeństwa informacji, w szczególności:
    a. dokonuje inwentaryzacji zasobów danych osobowych i dba o aktualność ich opisu zgodnie z wymogami określonymi w części III pkt. 2 ppkt. 2 niniejszej *Polityki*,
    b. przeprowadza ocenę ryzyka naruszenia ochrony danych osobowych
    c. jeśli to wymagane prowadzi rejestr czynności przetwarzania
    d. jeśli to wymagane przeprowadza ocenę skutków dla ochrony danych
    e. jeśli to wymagane prowadzi uprzednie konsultacje z organem nadzorczym
    f. czuwa nad aktualnością dokumentacji z zakresu ochrony danych osobowych
    g. czuwa nad przestrzegania zasad określonych w dokumentacji ochrony danych osobowych
    h. czuwa nad zgodnością przetwarzania danych osobowych z przepisami o ochronie danych osobowych
    i. prowadzi postępowanie wyjaśniające w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych
3) W celu realizacji zadań określonych w ppkt. 2 lit. f-h) pełnomocnik bezpieczeństwa informacji przeprowadza okresowe audyty wewnętrzne (tzw. sprawdzenia planowe). Realizując zadanie określone w ppkt. 2 lit. i pełnomocnik bezpieczeństwa informacji przeprowadza audyt wewnętrzny nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne).
4) Pełnomocnik bezpieczeństwa informacji wraz z administratorem danych zapewniają i nadzorują realizację obowiązku zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie tych danych, w szczególności decydują o terminach i sposobach przeprowadzenia szkoleń w tym zakresie.

2. Inwentaryzacja i opis zasobów

1) Pełnomocnik bezpieczeństwa informacji dba o to by przetwarzanie danych osobowych w TSLOGISTIC Tomasz Sawicki odbywało się wyłącznie za wiedzą, zgodą i pod nadzorem upoważnionych.
2) W celu realizacji zadania określonego w ppkt. 1) pełnomocnik bezpieczeństwa informacji opisuje zasoby danych osobowych oraz sposób ich przetwarzania i zabezpieczenia zgodnie z dokumentem *Opis zasobów danych osobowych.*
3) Pełnomocnik bezpieczeństwa informacji dba o aktualność opisu zasobów. Ocena aktualności opisu zasobów stanowi element okresowego przeglądu dokumentacji o którym mowa w pkt.8.

3. Rejestr czynności przetwarzania

1) TSLOGISTIC Tomasz Sawicki prowadzi rejestr czynności przetwarzania tak, by był on zgodny z wymogami art. 30 RODO. Przeprowadzając okresowy przegląd dokumentacji o którym mowa w pkt. 8 pełnomocnik bezpieczeństwa informacji dokonuje oceny spełnienia powyższego wymogu.

2) Pełnomocnik bezpieczeństwa informacji przekazuje rejestr czynności przetwarzania

organowi nadzorczemu na jego żądanie.

4. Ocena ryzyka

1) Celem oceny ryzyka jest ustalenie czy stopień bezpieczeństwa danych jest odpowiedni oraz czy nie zachodzi niebezpieczeństwo naruszenia praw i wolności osób fizycznych.
2) Administrator danych zleca pełnomocnikowi bezpieczeństwa informacji przeprowadzenie oceny ryzyka, gdy:
    a. są planowane lub podejmowane nowe czynności z wykorzystaniem danych osobowych,
    b. dokonywane są zmiany sposobu działania TSLOGISTIC Tomasz Sawicki, w szczególności zmiany w zakresie wykorzystywanej technologii i organizacji pracy, gdy może to mieć wpływ na przetwarzanie danych osobowych.
3) Wyniki oceny ryzyka pełnomocnik bezpieczeństwa informacji przedstawia niezwłocznie administratorowi danych. Jeśli na skutek przeprowadzonej oceny pełnomocnik bezpieczeństwa informacji ustali, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to administrator danych rezygnuje z planowanych działań, albo podejmuje czynności wskazane w ppkt. 4.
4) Jeśli administrator danych chce kontynuować planowane działania mimo, że z oceny ryzyka wynika, że z dużym prawdopodobieństwem mogą one powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to:
    a. zleca właściwym podmiotom, w tym pełnomocnikowi bezpieczeństwa informacji, opracowanie i zastosowanie środków zaradczych, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie postanowień RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy,
    b. zleca pełnomocnikowi bezpieczeństwa informacji przeprowadzenie oceny skutków przetwarzania dla ochrony danych osobowych zgodnie z pkt. 5.
    c. oceny skutków przetwarzania dla ochrony danych wskazanej w ppkt. 4 nie trzeba przeprowadzać, gdy przetwarzanie jest obowiązkiem wynikającym z przepisu prawa lub jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.
5) Ocenę ryzyka pełnomocnik bezpieczeństwa informacji przeprowadza także w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych zgodnie z częścią VIII niniejszej *Polityki.*

5. Ocena skutków przetwarzania dla ochrony danych

1) Jeżeli administrator danych osobowych zlecił pełnomocnikowi bezpieczeństwa informacji przeprowadzenie oceny skutków przetwarzania dla ochrony danych zgodnie z pkt. 4 ppkt. 4 lit. b), to pełnomocnik bezpieczeństwa informacji przystępuje niezwłocznie do opracowania takiej oceny.
2) Ocena skutków o której mowa w ppkt. 1) obejmuje:
    a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
    b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne stosunku do celów;

c. wskazanie środków zaplanowanych w celu zaradzenia ryzyku, ze szczególnym wyróżnieniem tych opracowanych i wdrożonych w ramach działań podjętych na zlecenie wskazane w pkt. 4 ppkt. 4 lit. a).

d. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, po zastosowaniu środków wskazanych w ppkt. 2 lit. c).

3) Wyniki oceny skutków pełnomocnik bezpieczeństwa informacji przedstawia niezwłocznie administratorowi danych. Jeśli ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby nadal wysokie ryzyko naruszenia wolności lub praw osób, których dane dotyczą, a zastosowane środki wskazane w pkt. 5 ppkt. 2 lit. c) nie pozwalają na jego zminimalizowanie, to administrator danych rezygnuje się z podejmowania planowanych działań, albo przedstawia sprawę organowi nadzorczemu w trybie uprzednich konsultacji zgodnie z pkt. 6.

6. Uprzednie konsultacje z organem nadzorczym

1) Jeśli w sytuacji określonej w pkt. 5 ppkt. 3) administrator danych podejmie decyzję o przeprowadzeniu uprzednich konsultacji z organem nadzorczym nakazuje pełnomocnikowi bezpieczeństwa informacji przygotowanie odpowiedniej dokumentacji dla tego organu.

2) Informacja przygotowana dla organu nadzorczego obejmuje:

a. wskazanie celów i sposobów zamierzonego przetwarzania,

b. wskazanie środków i zabezpieczeń mających chronić prawa i wolności osób, których dane dotyczą,

c. kopię oceny skutków dla ochrony danych, o której mowa w pkt. 5.

3. Jeśli administrator przetwarza dane osobowe wspólnie z innymi podmiotami, w szczególności w ramach grupy przedsiębiorstw, to informacja przygotowana dla organu nadzorczego zawiera dodatkowo wskazanie obowiązków poszczególnych administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu.

3) Administrator danych stosuje się do zaleceń wydanych przez organ nadzorczy w ramach konsultacji. Jeśli organ nadzorczy wystąpi z żądaniem udzielenia dodatkowych informacji to administrator zleca ich przygotowanie pełnomocnikowi bezpieczeństwa informacji.

7. Audyty wewnętrzne

1) W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych pełnomocnik bezpieczeństwa informacji przeprowadza następujące audyty wewnętrzne:

- sprawdzenie prawidłowości i aktualności dokumentacji z zakresu ochrony danych osobowych;

- sprawdzenie przestrzegania zasad i procedur określonych w dokumentacji ochrony danych osobowych.

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) Audyty wewnętrzne wskazane w ppkt. 1) są przeprowadzane okresowo zgodnie z planem sprawdzeń przygotowywanym przez pełnomocnika bezpieczeństwa informacji (sprawdzenia planowe). Plan sprawdzeń obejmuje maksimum 1 rok. Jest on przekazywany administratorowi danych do wiadomości w terminie minimum 2 tygodni przed rozpoczęciem okresu, który plan obejmuje. Jeśli sprawdzenie planowe obejmuje kontrolę w konkretnej jednostce lub dziale to kierownik tej jednostki jest

zawiadamiany o sprawdzeniu nie później niż na 7 dni przed rozpoczęciem sprawdzenia.

3) W sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia pełnomocnik bezpieczeństwa informacji przeprowadza audyt nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne). W przypadku sprawdzeń doraźnych terminy określone w ppkt. 2) nie obowiązują.

4) Pełnomocnik bezpieczeństwa informacji przygotowuje i gromadzi dokumentację przeprowadzonych audytów.

5) Obowiązki określone w ppkt. 1-4) pełnomocnik bezpieczeństwa informacji realizuje we współpracy z administratorem systemu oraz administratorem danych.

8. Zapewnienie aktualności dokumentacji z zakresu ochrony danych osobowych

1) Pełnomocnik bezpieczeństwa informacji dokłada starań by dokumentacja ochrony danych osobowych była aktualna. W tym celu na bieżąco śledzić zmiany stanu prawnego oraz zapoznaje się z treścią wytycznych i wskazówek wydawanych przez organ nadzorczy w tym zakresie.

2) Niezależnie od działań wskazanych w ppkt. 1) pełnomocnik bezpieczeństwa informacji nie rzadziej niż raz na półtora roku dokonuje przeglądu dokumentacji pod kątem sprawdzenia jej aktualności i zgodności z przepisami.

9. Zapewnienie przestrzegania zasad określonych w dokumentacji ochrony danych osobowych.

1) Pełnomocnik bezpieczeństwa informacji prowadzi bieżący nadzór nad działalnością TSLOGISTIC Tomasz Sawicki związaną z przetwarzaniem danych osobowych. Realizując powyższe zadanie pełnomocnik bezpieczeństwa informacji m. in. na bieżąco ocenia zagrożenia, sprawdza kluczowe punkty bezpieczeństwa, formułuje zalecenia i wskazówki, odpowiada na pytania i udziela porad.

2) Niezależnie od działań wskazanych w ppkt. 1) pełnomocnik bezpieczeństwa informacji nie rzadziej niż raz do roku przeprowadza audyt przestrzegania zasad i procedur ochrony danych osobowych w TSLOGISTIC Tomasz Sawicki.

3) W ramach audytu określonego w ppkt. 2) dokonuje się w szczególności analizy zagrożeń określonych w części IV niniejszej *Polityki* oraz sprawdza realizację wskazań i obowiązków określonych w części V niniejszej *Polityki*.

10. Zapewnienie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

1) Pełnomocnik bezpieczeństwa informacji na bieżąco śledzi zmiany prawne i zapoznaje się ze wskazówkami organu nadzorczego wydanymi w zakresie ich wdrożenia. Pełnomocnik bezpieczeństwa informacji informuje administratora danych o planowanych zmianach prawnych i w porozumieniu z nim oraz, gdy to właściwe, z udziałem administratora systemu, przygotowuje projekty dostosowujące działania, zasady i procedury wewnętrzne do nowych wymogów.

2) Niezależnie od działań wskazanych w ppkt. 1) pełnomocnik bezpieczeństwa informacji nie rzadziej niż raz do roku przeprowadza audyt zgodności przetwarzania danych osobowych z przepisami TSLOGISTIC Tomasz Sawicki.

3) W ramach audytu określonego w ppkt. 2) dokonuje się w szczególności oceny realizacji wymogów wskazanych w części VI niniejszej *Polityki.*

VIII. Naruszenie ochrony danych osobowych.

1. Postępowanie w przypadku stwierdzenia lub podejrzenia stwierdzenia naruszenia ochrony danych osobowych

1) Zasady postępowania w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego określa *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w TSLOGISTIC Tomasz Sawicki.*
2) Każdy kto stwierdził inne niż określone w ppkt. 1) naruszenie ochrony danych osobowych lub podejrzewa takie naruszenie powinien niezwłocznie poinformować o tym pełnomocnika bezpieczeństwa informacji lub administratora danych. Jako inne niż określone w ppkt. 1) naruszenie rozumie się w szczególności brak realizacji lub niewłaściwą realizację wymogów określonych w części VI niniejszej *Polityki*.
3) Pełnomocnik bezpieczeństwa informacji po otrzymaniu zawiadomienia, o którym mowa w ppkt. 2) przeprowadza niezwłocznie postępowanie wyjaśniające w celu ustalenia czy naruszenie ochrony danych osobowych miało miejsce (tzw. sprawdzenie doraźne).
4) Sprawdzenie doraźne może zostać wszczęte przez pełnomocnik bezpieczeństwa informacji także z własnej inicjatywy, gdy w inny sposób niż w skutek zawiadomienia poweźmie informację o naruszeniu lub możliwym naruszeniu ochrony danych osobowych.
5) W przypadku stwierdzenia naruszenia ochrony danych osobowych w trybie określonym w ppkt. 3 lub 4) pełnomocnik bezpieczeństwa informacji:
    a. w porozumieniu z odpowiednim kierownikiem działu podejmuje niezwłoczne, możliwe do wprowadzenia na bieżąco, działania zapobiegające dalszemu naruszaniu ochrony danych osobowych,
    b. w porozumieniu z odpowiednim kierownikiem działu stosuje niezwłoczne, możliwe do wprowadzenia na bieżąco, środki eliminujące lub zmniejszające ryzyko naruszenia praw lub wolności osoby, której dane dotyczą,
    c. sporządza raport naruszenia ochrony danych osobowych, a następnie niezwłocznie przekazuje jego kopię administratorowi danych.
6) Raport o którym mowa w ppkt. 5 lit. c) zawiera w szczególności:
    a. opis okoliczności naruszenia ochrony danych osobowych;
    b. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    c. opis możliwych konsekwencji naruszenia ochrony danych osobowych;
    d. ocenę czy jest prawdopodobne, że naruszenie skutkowało ryzykiem lub wysokim ryzykiem naruszenia wolności lub praw osób fizycznych;
    e. wskazanie zastosowanych lub proponowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które zmierzają do zminimalizowania ewentualnych negatywnych skutków naruszenia.
7) Administrator danych osobowych po zapoznaniu się z raportem o którym mowa w ppkt. 6) podejmuje decyzje o dalszym trybie postępowania, a w szczególności:
    a. jeśli to właściwe, zarządza podjęcie czynności zmierzających do usunięcia naruszenia i jego skutków oraz zapobieżeniu naruszeniom ochrony danych osobowych na przyszłość.

b. jeśli to możliwe, zarządza zastosowanie środków eliminujących lub zmniejszających prawdopodobieństwo ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c. jeśli jest to właściwe zawiadamia o naruszeniu właściwe organy, w tym zgłasza naruszenie organowi nadzorczemu oraz informuje o naruszeniu osoby, których naruszenie dotyczy. Zgłasza naruszenie organowi nadzorczemu zgodnie z art. 33 ust. 1 RODO oraz zawiadamia o naruszeniu osób, których dane dotyczą zgodnie z art. 34 ust. 1 RODO stosuje się postanowienia pkt. 2 i 3 niniejszej części,.

2. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu i zawiadomienie osoby, której dane dotyczą.

1) Jeśli administrator danych ustali, że jest prawdopodobne, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w pkt. 1 skutkowało ryzykiem naruszenia wolności lub praw osób fizycznych nakazuje pełnomocnikowi bezpieczeństwa informacji przygotowanie projektu zgłoszenia naruszenia organowi nadzorczemu,

2) Zgłoszenie naruszenia wskazane w ppkt. 1) zawiera, w szczególności:

   a. informacje zawarte w raporcie, zgodnie z pkt. 1 ppkt. 6),

   b. wskazanie imienia i nazwiska oraz danych kontaktowych pełnomocnika bezpieczeństwa informacji, jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych osobowych, do kontaktu w sprawie może być wskazana inna osoba niż pełnomocnik bezpieczeństwa informacji.

3) Zgłoszenie naruszenia ochrony danych osobowych, o którym mowa w ppkt. 1-2) administrator danych zatwierdza i przekazuje organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

4) Jeżeli dotrzymanie terminu wskazanego w ppkt. 3) jest niemożliwe administrator danych do zgłoszenia dołącza wyjaśnienie przyczyn opóźnienia. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić od razu, administrator danych udziela tych informacji sukcesywnie, bez zbędnej zwłoki.

3. Zawiadomienie osoby, której dane dotyczą.

1) Jeśli administrator danych ustali, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w pkt. 1 może powodować wysokie ryzyko naruszenia wolności lub praw osób fizycznych i nie da się zastosować środków eliminujących to wysokie ryzyko, nakazuje pełnomocnikowi bezpieczeństwa informacji przygotowanie projektu zawiadomienia o naruszeniu dla wszystkich osób, których danych naruszenie dotyczy.

2) Zawiadomienie o którym mowa w ppkt. 1) powinno być napisane jasnym i prostym językiem oraz zawierać, w szczególności:

   a. opis charakteru naruszenia,

   b. opis możliwych konsekwencji naruszenia,

   c. wskazanie zastosowanych lub planowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które mogą zminimalizować ewentualne negatywne skutki naruszenia,

   d. wskazanie imienia i nazwiska oraz danych kontaktowych pełnomocnika

bezpieczeństwa informacji, jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych osobowych, do kontaktu w sprawie może być wskazana inna osoba niż pełnomocnik bezpieczeństwa informacji.

3) Zawiadomienie o naruszeniu ochrony danych osobowych, o którym mowa w ppkt. 1-2) administrator danych zatwierdza i przekazuje niezwłocznie wszystkim osobom, których danych naruszenie dotyczy.

4) Jeżeli administrator danych oceni, że realizacja wymogów określonych w ppkt. 1-3) wymagałoby niewspółmiernie dużego wysiłku, w szczególności niewspółmiernie dużego wysiłku wymagałoby nawiązanie bezpośredniego, indywidualnego kontaktu z osobami, których danych naruszenie dotyczy, może podjąć decyzje o przekazaniu informacji zainteresowanym poprzez wydanie publicznego komunikatu lub o zastosowaniu innego podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Dokumentacja naruszenia ochrony danych osobowych.

1) Pełnomocnik bezpieczeństwa informacji prowadzi dokumentację naruszenia danych osobowych.

2) W skład dokumentacji o której mowa w ppkt. 1) wchodzą:
   a. kopia raportu o którym mowa w pkt. 1 ppkt. 6,
   b. kopia zgłoszenia o którym mowa w pkt. 2
   c. kopie zawiadomień o których mowa w pkt. 3
   d. wszelkie inne dokumenty, w tym notatki służbowe, pliki, zdjęcia i inne dowody zebrane w trakcie przeprowadzania czynności wyjaśniających pozwalające ustalić okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

3) Dokumentacja naruszenia ochrony danych osobowych pozostaje do wglądu organu nadzorczego.

IX. Postanowienia końcowe

1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się i stosować do zasad i procedur określonych w niniejszej *Polityce*.

2) Naruszenie zasad i procedur określonych w niniejszej *Polityce* może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

3) Naruszenie zasad i procedur określonych w niniejszej *Polityce* może być potraktowane jako nienależyte wykonanie umowy w rozumieniu Kodeksu cywilnego.

4) *Polityka ochrony danych osobowych w TSLOGISTIC Tomasz Sawicki* wchodzi w życie z dniem ogłoszenia.