POLITYKA OCHRONY DANYCH OSOBOWYCH

IMPEX-READY Spółka Cywilna Artur Markiewicz, Marcin Kaczyński

z/s ul. Wolności 135A, 42-460 Mierzęcice

NIP: 6262856685, REGON: 240604522

z dnia 24 maja 2018 r.

I. Postanowienia wprowadzające

1. Cele i deklaracje

1) Wspólnicy administratora danych, świadomi wagi zagrożeń jakie niesie ze sobą przetwarzanie danych osobowych dla wolności i praw osób, których dane dotyczą, uznają ochronę tych danych, w szczególności zapewnienie ich bezpieczeństwa, za jeden z priorytetów działalności IMPEX-READY Spółka Cywilna Artur Markiewicz, Marcin Kaczyński (dalej: IMPEX-READY S.C.)
2) Wspólnicy administratora danych podejmują działania mające na celu wdrożenie przez IMPEX-READY S.C. przepisów o ochronie danych osobowych oraz zapewnienie stałej zgodności działalności IMPEX-READY S.C. z tymi przepisami.
3) W celu realizacji zadań określonych w ppkt. 1) i 2) ustanawia się *Politykę ochrony danych osobowych w* IMPEX-READY S.C. 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) Wspólnicy administratora danych oczekują, 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 IMPEX-READY S.C. 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 IMPEX-READY S.C., zarówno do zatrudnionych IMPEX-READY S.C., 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 IMPEX-READY Spółka Cywilna Artur Markiewicz, Marcin Kaczyński reprezentowaną przez wspólników, stosownie do § 7 Umowy Spółki Cywilnej z dnia 21.03.2007 r. ze zm. wprowadzonymi aneksami z dni: 26.10.2016 r. i 30.11.2017 r.
2) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
3) identyfikatorze – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
4) integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione, usunięte lub zniszczone w sposób nieautoryzowany,
5) 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,
6) poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
7) podmiocie przetwarzającym – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 28 RODO,
8) raportach – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
9) RODO – rozumie się przez to rozporządzenie 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,
10) rozliczalności – rozumie się przez to właściwość zapewniającą, że podejmowane działania mogą być przypisane w sposób jednoznaczny konkretnej osobie lub podmiotowi,
11) 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. Dz. U. z 2017 r., poz. 1907 ze zm.),
12) serwisancie – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,
13) 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,

14) ustawie – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000),

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

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

17) użytkowniku – rozumie się przez to upoważnionego, któremu nadano identyfikator i przyznano hasło.

II. Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

Administrator danych osobowych (dalej: administrator danych), reprezentowany przez wspólników, 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) prowadzi ewidencję 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) zapewnia użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;

5) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;

6) realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym, w tym zwłaszcza:

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

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

   c) 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,

   d) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli

dostępu do danych osobowych,

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

f) wyrejestrowuje użytkowników,

g) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi,

h) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,

i) 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,

j) 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.

2. 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 nań obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy lub 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 *Polityki bezpieczeństwa danych osobowych w* IMPEX-READY S.C. oraz *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*;

4) stosuje się do wydawanych przez administratora danych 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 załącznik ***Opis obszaru przetwarzania***.

2. Zasoby danych osobowych

1) Na zasoby danych osobowych IMPEX-READY S.C. 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 IMPEX-READY S.C. obejmujący informację o treści i strukturze każdego z zasobów oraz o sposobie przepływu danych pomiędzy zasobami określa załącznik ***Opis zasobów danych osobowych***.

3. System informatyczny

Sposób przetwarzania danych osobowych w systemie informatycznym administratora danych określają załączniki ***Opis zasobów danych osobowych*** oraz ***Ewidencja czynności przetwarzania***.

4. Dokumentacja ochrony danych osobowych

1) IMPEX-READY S.C. 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 pkt. 4 ppkt. 2),
    d) rejestr czynności przetwarzania,
    e) dokumentacja audytów o której mowa w pkt. 4 ppkt. 3),
    f) umowy z podmiotami przetwarzającymi (jeśli zostaną zawarte),
    g) umowy z współadministratorami (jeśli zostaną zawarte);
2) w ramach dokumentacji ochrony danych osobowych prowadzone są następujące ewidencje:
    a) ewidencja osób upoważnionych do przetwarzania danych osobowych,
    b) ewidencja udostępnień danych osobowych,
    c) ewidencja użytkowników systemu informatycznego, a także ewidencja komputerów przenośnych;
3) na dokumentację audytów, których mowa w ppkt. 1 lit. e) składają się:
    a) dokumentacja sprawdzeń planowych przeprowadzonych zgodnie z postanowieniami części VII pkt. 7 ppkt. 1 niniejszej *Polityki*.
    b) dokumentacja sprawdzeń doraźnych zgodna z postanowieniami części VIII pkt. 4.

IV. Identyfikacja zagrożeń bezpieczeństwa danych osobowych

Identyfikuje się następujące zagrożenia bezpieczeństwa danych osobowych przetwarzanych przez IMPEX-READY S.C.:

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 tego ostatniego,
    - 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, niezamknięcie na klucz pokoju po jego opuszczeniu),
    - 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 I, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli. W skład tej strefy wchodzą:
   a) pomieszczenie z serwerem („serwerownia"), w którym mogą przebywać wyłącznie wspólnicy, inne osoby upoważnione do przetwarzania tylko w towarzystwie wspólników, a osoby postronne w ogóle nie mają dostępu;
   b) pomieszczenie księgowości („księgowość"), w którym może przebywać wyłącznie księgowa, inni użytkownicy danych tylko w towarzystwie księgowej, 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) Serwer jest zlokalizowany w odrębnym pomieszczeniu, zabezpieczonym drzwiami zamykanymi na klucz.
2) Wspólnicy wskazują użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację urządzeń i systemu informatycznego.
3) Wszystkie urządzenia systemu informatycznego administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).
4) 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.
5) Bieżąca konserwacja sprzętu administratora danych wykorzystywanego do przetwarzania danych osobowych prowadzona jest przez wspólników lub pod ich nadzorem przez innych upoważnionych.
6) W przypadku konieczności dokonania naprawy przez podmiot zewnętrzny, w siedzibie administratora danych, dokonuje się tego po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych lub po usunięciu tych danych.
7) W szczególnych przypadkach, gdy nie istnieje ryzyko naruszenia ochrony danych osobowych, można dokonać naprawy w warunkach określonych w ppkt. 6) bez zawarcia umowy o powierzeniu przetwarzania danych i bez usunięcia danych, jednak pod ścisłym nadzorem wspólnika dbającego o to, by serwisant nie miał dostępu do danych osobowych administratora danych.
8) Administrator danych dopuszcza konserwowanie i naprawę sprzętu poza swoją

siedzibą jedynie po trwałym usunięciu danych osobowych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych.

9) 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. Dostęp do niego jest jednak ograniczony.
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 danych. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora danych oraz umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.
4) Administrator 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 danych, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.
2) W razie potrzeby administrator danych może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.
3) Administrator danych przeprowadza synchronizację zegarów stacji roboczych z serwerem, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez administratora danych z konta o uprawnieniach administracyjnych.

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 bezpieczeństwa informacji*, 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 osobowy 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) przekazywania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

13) zapisywanie plików lub wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

14) 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;

15) 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);

16) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;

17) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

18) zamykania drzwi na klucz po zakończeniu pracy w danym dniu i przekazania klucza jednemu ze wspólników.

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, gdy konieczność taka została z tym ostatnim uzgodniona.

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 danych 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 IMPEX-READY S.C. 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) - w art. 9 i art. 10 RODO.

2) **Zasada rzetelności przetwarzania**. Przetwarzanie rzetelne należy rozumieć jako przetwarzanie uczciwie w stosunku do osoby, których dane dotyczą. 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**, 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 jednego miesiąca, chyba że sprawa jest skomplikowana. Wtedy przedłużenie terminu następuje zgodnie 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**, 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 administrator danych.

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, opisuje się 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 międzynarodowych

1) Przekazywanie danych osobowych do państw trzecich jest zasadniczo zabronione, 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 danych osobowych oraz sposobu 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, zapewnia się zgodność działalności IMPEX-READY S.C. z przepisami.

2) Realizując zadanie określone w ppkt. 1) administrator danych, 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 przestrzeganiem 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) administrator danych przeprowadza okresowe audyty wewnętrzne (tzw. sprawdzenia planowe). Realizując zadanie określone w ppkt. 2 lit. i administrator danych przeprowadza audyt wewnętrzny nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne).
4) Administrator danych zapewnia (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.

2. Inwentaryzacja i opis zasobów

1) Administrator danych dba o to, by przetwarzanie danych osobowych w IMPEX-READY S.C. odbywało się wyłącznie za wiedzą, zgodą i pod nadzorem upoważnionych.
2) W celu realizacji zadania określonego w ppkt. 1), administrator danych opisuje zasoby danych osobowych oraz sposób ich przetwarzania i zabezpieczenia zgodnie z załącznikiem ***Opis zasobów danych osobowych***.
3) Administrator danych 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) IMPEX-READY S.C. prowadzi rejestr czynności przetwarzania tak, by był on zgodny z wymogami art. 30 RODO. Przeprowadzając okresowy przegląd dokumentacji, o którym mowa w pkt. 8, administrator danych dokonuje oceny spełnienia powyższego wymogu.
2) Administrator danych 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 wolności i praw osób fizycznych.
2) Administrator danych przeprowadza ocenę ryzyka, gdy:
    a. są planowane lub podejmowane nowe czynności z wykorzystaniem danych osobowych,
    b. dokonywane są zmiany sposobu działania IMPEX-READY S.C., w szczególności zmiany w zakresie wykorzystywanej technologii i organizacji pracy, gdy może to mieć wpływ na przetwarzanie danych osobowych.
3) Jeśli na skutek przeprowadzonej oceny administrator danych ustali, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia wolności lub praw 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 wolności lub praw osób fizycznych, to:
    a. zleca właściwym podmiotom 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. przeprowadza ocenę 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 przeprowadza się 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) Ocena skutków 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 wolności lub praw osób, których dane dotyczą, po zastosowaniu środków wskazanych w ppkt. 1 lit. c).

2) 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. 1 lit. c) nie pozwalają na jego zminimalizowanie, to administrator danych rezygnuje 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. 2) administrator danych podejmie decyzję o przeprowadzeniu uprzednich konsultacji z organem nadzorczym nakazuje 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 wolności i prawa 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 upoważnionemu ku temu pracownikowi.

7. Audyty wewnętrzne

1) W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych administrator danych 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 przygotowanym przez upoważnionego pracownika (sprawdzenia planowe). Plan sprawdzeń obejmuje maksimum 1 rok.

3) W sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia administrator danych przeprowadza audyt nieobjęty planem sprawdzeń (tzw. sprawdzenie doraźne).

4) Administrator danych przygotowuje i gromadzi dokumentację przeprowadzonych audytów.

8. Zapewnienie aktualności dokumentacji z zakresu ochrony danych osobowych

1) Administrator danych dokłada starań, by dokumentacja ochrony danych osobowych była aktualna. W tym celu na bieżąco śledzi 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), administrator danych dokonuje przeglądu dokumentacji pod kątem sprawdzenia jej aktualności i zgodności z przepisami.

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

1) Administrator danych prowadzi bieżący nadzór nad działalnością IMPEX-READY S.C. związaną z przetwarzaniem danych osobowych. Realizując powyższe zadanie 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) administrator danych, nie rzadziej niż raz do roku, przeprowadza audyt przestrzegania zasad i procedur ochrony danych osobowych w IMPEX-READY S.C.

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) Administrator danych na bieżąco śledzi zmiany prawne i zapoznaje się ze wskazówkami organu nadzorczego wydanymi w zakresie ich wdrożenia. Przygotowuje projekty dostosowujące działania, zasady i procedury wewnętrzne do nowych wymogów.

2) Niezależnie od działań wskazanych w ppkt. 1) administrator danych nie rzadziej niż raz do roku przeprowadza audyt zgodności przetwarzania danych osobowych z przepisami IMPEX-READY S.C.

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 IMPEX-READY S.C.

2) Każdy, kto stwierdził inne niż określone w ppkt. 1) naruszenie ochrony danych osobowych lub podejrzewa takie naruszenie powinien niezwłocznie poinformować o tym 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) Administrator danych 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 administratora danych 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) administrator danych:
    a) podejmuje niezwłoczne, możliwe do wprowadzenia na bieżąco, działania zapobiegające dalszemu naruszaniu ochrony danych osobowych,
    b) 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 sporządzeniu raportu, 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. Do zgłasza naruszenia 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 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 upoważnionego pracownika, jako osoby właściwej do kontaktu w sprawie.
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, przygotowuje projekt 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 upoważnionego pracownika, jako osoby właściwej do kontaktu w sprawie.
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) Administrator danych 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. Przepisy przejściowe

1) Niniejsza *Polityka ochrony danych osobowych* IMPEX-READY S.C. zastępuje *Politykę bezpieczeństwa informacji* z *dnia* 12 maja 2014 r.

2) Wszyscy przetwarzający dane osobowe w IMPEX-READY S.C. zobowiązani są dostosować swoje działania do wymogów niniejszej *Polityki* niezwłocznie, nie później jednak niż do 25 maja 2018 r.

3) Administrator danych niezwłocznie po wejściu w życie niniejszej polityki podejmie działania w celu dostosowania lub opracowania wszystkich dokumentów, ewidencji, wzorów i formularzy wynikających z niniejszej *Polityki*.

4) Pierwsze audyty planowe o których mowa w części VII pkt. 7 ppkt. 1) zostaną przeprowadzone w takim terminie, by wynikające z nich zalecenia i wnioski można było wprowadzić w życie przed 25 maja 2018 r.

X. 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 IMPEX-READY S.C. wchodzi w życie z dniem ogłoszenia.